

Docket No. 200133US2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Yoichi KANAI, et al.

GAU: 2142

SERIAL NO: 09/725,515

EXAMINER: VU, THONG, H.

FILED: November 30, 2000

FOR: SYSTEM, METHOD AND COMPUTER READABLE MEDIUM FOR
CERTIFYING RELEASE OF ELECTRONIC INFORMATION ON AN
INTERNET

SUBMISSION NOTICE REGARDING PRIORITY DOCUMENT(S)

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

Certified copies of the Convention Application(s) corresponding to the above-captioned matter:

☒ are submitted herewith

☐ were filed in prior application filed

☐ were submitted to the International Bureau in PCT Application Number _____
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule
17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Registration No. 25,599

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 11/04)

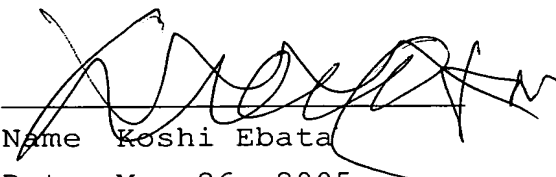
I:\ATTY\SNS\20's\200133\SUBMISSION NOTICE OF PRIORITY 06.04.05.doc

Surinder Sachar
Registration No. 34,423



CERTIFICATE OF TRANSLATOR

I, Koshi Ebata of Kashimada 118, Saiwai-ku, Kawasaki-shi, Kanagawa-ken, Japan do hereby declare that I am well acquainted with the Japanese and English languages and that the attached English translation is a true translation from the Japanese into English of Japanese Patent Application Nos. 1999-341288 and 1999-341289 both filed with the Japanese Patent Office on November 30, 1999.


Name Koshi Ebata
Date May 26, 2005

BEST AVAILABLE COPY

CERTIFIED COPY OF
PRIORITY DOCUMENT

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日
Date of Application:

1999年11月30日

願 番 号
Application Number:

平成11年特許願第341289号

条約による外国への出願
する優先権の主張の基礎
となる出願の国コードと出願

country code and number
of our priority application,
used for filing abroad
under the Paris Convention, is

J P 1 9 9 9 - 3 4 1 2 8 9

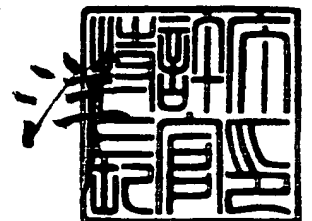
願 人
Applicant(s):

株式会社リコー

2005年 5月 2日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願

【整理番号】 9907602

【提出日】 平成11年11月30日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00
G06F 12/14

【発明の名称】 電子情報公開証明方法及びシステム、並びに電子情報公開証明プログラムを格納した記憶媒体

【請求項の数】 14

【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号
株式会社 リコー内

【氏名】 谷内田 益義

【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号
株式会社 リコー内

【氏名】 金井 洋一

【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号
株式会社 リコー内

【氏名】 水野 富夫

【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号
株式会社 リコー内

【氏名】 古川 達也

【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号
株式会社 リコー内

【氏名】 石川 洋一

【特許出願人】**【識別番号】** 000006747**【氏名又は名称】** 株式会社 リコー**【代表者】** 桜井 正光**【手数料の表示】****【予納台帳番号】** 003724**【納付金額】** 21,000円**【提出物件の目録】****【物件名】** 明細書 1**【物件名】** 図面 1**【物件名】** 要約書 1**【プルーフの要否】** 要

【書類名】 明細書

【発明の名称】 電子情報公開証明方法及びシステム、並びに電子情報公開証明プログラムを格納した記憶媒体

【特許請求の範囲】

【請求項 1】 ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明する方法であって、

記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報にアクセスし、前記特定の電子情報及び当該特定の電子情報にオブジェクトが含まれる場合には当該オブジェクトをコピーする第 1 ステップと、

前記特定の電子情報及び前記オブジェクトをローカルに保存した場合にローカルに保存された前記特定の電子情報から前記オブジェクトを利用可能なように前記特定の電子情報を変更し、変更された前記特定の電子情報をコピーされた前記オブジェクトと共に記憶装置に格納する第 2 ステップと、

コピーされた前記特定の電子情報及び前記オブジェクトと、変更された前記特定の電子情報と、前記ネットワーク上における前記特定の電子情報の所在に関する情報を含む属性情報とを日時と共にユニークに特定し且つ認証する電子証明書を取得する第 3 ステップと、

変更された前記特定の電子情報に対応して、前記電子証明書及び前記属性情報を記憶装置に格納する第 4 ステップと、

を含むことを特徴とする電子情報公開証明方法。

【請求項 2】 コピーされた前記特定の電子情報を記憶装置に格納する第 5 ステップをさらに含むことを特徴とする請求項 1 記載の電子情報公開証明方法。

【請求項 3】 前記記憶装置に格納された、前記電子証明書と前記属性情報と変更された前記電子情報と前記オブジェクトとを証明依頼元に提供する第 6 ステップをさらに含むことを特徴とする請求項 1 記載の電子情報公開証明方法。

【請求項 4】 前記特定の電子情報から参照される第 2 の電子情報又は第 2 のオブジェクトにアクセスし、前記第 2 の電子情報又は第 2 のオブジェクトをコピーする第 7 ステップをさらに含み、

前記第 2 ステップは、

前記特定の電子情報及び前記オブジェクト並びに前記第 2 の電子情報又は前記第 2 のオブジェクトをローカルに保存した場合にローカルに保存された前記特定の電子情報から前記オブジェクト並びに前記第 2 の電子情報又は前記第 2 のオブジェクトを利用可能なように前記特定の電子情報を変更するステップを含み、

前記第 3 ステップは、

コピーされた前記特定の電子情報及び前記オブジェクト並びに前記第 2 の電子情報又は前記第 2 のオブジェクトと、変更された前記特定の電子情報と、前記ネットワーク上における前記特定の電子情報の所在に関する情報を含む属性情報とを日時と共にユニークに特定し且つ認証する電子証明書を取得するステップであることを特徴とする請求項 1 記載の電子情報公開証明方法。

【請求項 5】 前記ネットワークがインターネットであり、

前記電子情報はマークアップ・ランゲージにより記述された文書であり、

前記ネットワーク上における前記電子情報の所在に関する情報はユニフォーム・リソース・ロケータであり、

前記電子情報に含まれるオブジェクトは、静止画像、動画像、サウンド、アプレット、又は前記電子情報により指定されたフォーマットのデータであることを特徴とする請求項 1 記載の電子情報公開証明方法。

【請求項 6】 ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明する方法であって、

記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報にアクセスし、前記特定の電子情報及び当該特定の電子情報が第 2 の電子情報又はオブジェクトを参照している場合には当該第 2 の電子情報又はオブジェクトをコピーする第 1 ステップと、

前記特定の電子情報及び前記第 2 の電子情報又はオブジェクトをローカルに保存した場合にローカルに保存された前記特定の電子情報から前記第 2 の電子情報又はオブジェクトを利用可能なように前記特定の電子情報を変更し、変更された前記特定の電子情報をコピーされた前記第 2 の電子情報又はオブジェクトと共に記憶装置に格納する第 2 ステップと、

コピーされた前記特定の電子情報及び前記第 2 の電子情報又はオブジェクトと、変更された前記特定の電子情報と、前記ネットワーク上における前記特定の電子情報の所在に関する情報を含む属性情報とを日時と共にユニークに特定し且つ認証する電子証明書を取得する第 3 ステップと、

変更された前記特定の電子情報に対応して、前記電子証明書及び前記属性情報を記憶装置に格納する第 4 ステップと、

を含むことを特徴とする電子情報公開証明方法。

【請求項 7】 ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明するシステムであって、

記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報にアクセスし、前記特定の電子情報及び当該特定の電子情報に含まれるオブジェクトをコピーするアクセス手段と、

前記特定の電子情報及び前記オブジェクトをローカルに保存した場合にローカルに保存された前記特定の電子情報から前記オブジェクトを利用可能なように前記特定の電子情報を変更し、変更された前記特定の電子情報をコピーされた前記オブジェクトと共に記憶装置に格納する変更手段と、

コピーされた前記特定の電子情報と、コピーされた前記オブジェクトと、変更された前記特定の電子情報と、前記ネットワーク上における前記特定の電子情報の所在に関する情報を含む属性情報とを日時と共にユニークに特定し且つ認証する電子証明書を取得し、変更された前記特定の電子情報に対応して、前記電子証明書及び前記属性情報を記憶装置に格納する電子証明書取得手段と、

前記記憶装置に格納された前記電子証明書と、前記属性情報と、変更された前記電子情報と、前記オブジェクトとを証明依頼元に提供する手段と、

を有する電子情報公開証明システム。

【請求項 8】 前記アクセス手段が、コピーされた前記特定の電子情報を記憶装置に格納することを特徴とする請求項 7 記載の電子情報公開証明システム。

【請求項 9】 前記電子証明書を発行する手段をさらに有することを特徴とする請求項 7 記載の電子情報公開証明システム。

【請求項 10】 前記アクセス手段が、前記特定の電子情報から参照される

第 2 の電子情報又は第 2 のオブジェクトにアクセスし、前記第 2 の電子情報又は第 2 のオブジェクトをコピーし、

前記変更手段が、前記特定の電子情報及び前記オブジェクト並びに前記第 2 の電子情報又は前記第 2 のオブジェクトをローカルに保存した場合にローカルに保存された前記特定の電子情報から前記オブジェクト並びに前記第 2 の電子情報又は前記第 2 のオブジェクトを利用可能なように前記特定の電子情報を変更し、

前記電子証明書取得手段が、コピーされた前記特定の電子情報及び前記オブジェクト並びに前記第 2 の電子情報又は前記第 2 のオブジェクトと、変更された前記特定の電子情報と、前記ネットワーク上における前記特定の電子情報の所在に関する情報を含む属性情報とを日時と共にユニークに特定し且つ認証する電子証明書を取得することを特徴とする請求項 7 項記載の電子情報公開証明システム。

【請求項 1 1】 前記ネットワークがインターネットであり、前記電子情報はマークアップ・ランゲージにより記述された文書であり、

前記ネットワーク上における前記電子情報の所在に関する情報はユニフォーム・リソース・ロケータであり、

前記電子情報に含まれるオブジェクトは、静止画像、動画像、サウンド、アプレット、又は前記電子情報により指定されたフォーマットのデータであることを特徴とする請求項 7 記載の電子情報公開証明システム。

【請求項 1 2】 ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明するシステムであって、

記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報にアクセスし、前記特定の電子情報及び当該特定の電子情報が第 2 の電子情報又はオブジェクトを参照している場合には当該第 2 の電子情報又はオブジェクトをコピーする手段と、

前記特定の電子情報及び前記第 2 の電子情報又はオブジェクトをローカルに保存した場合にローカルに保存された前記特定の電子情報から前記第 2 の電子情報又はオブジェクトを利用可能なように前記特定の電子情報を変更し、変更された前記特定の電子情報をコピーされた前記第 2 の電子情報又はオブジェクトと共に記憶装置に格納する手段と、

コピーされた前記特定の電子情報及び前記第 2 の電子情報又はオブジェクトと、変更された前記特定の電子情報と、前記ネットワーク上における前記特定の電子情報の所在に関する情報を含む属性情報とを日時と共にユニークに特定し且つ認証する電子証明書を取得し、変更された前記特定の電子情報に対応して、前記電子証明書及び前記属性情報を記憶装置に格納する手段と、

前記記憶装置に格納された前記電子証明書と、前記属性情報と、変更された前記電子情報と、前記第 2 の電子情報又はオブジェクトとを証明依頼元に提供する手段と、

を有する電子情報公開証明システム。

【請求項 1 3】 ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明するためのプログラムを格納した記憶媒体であって、

前記プログラムは、前記特定のコンピュータ以外のコンピュータに、

記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報にアクセスし、前記特定の電子情報及び当該特定の電子情報に含まれるオブジェクトをコピーする第 1 ステップと、

前記特定の電子情報及び前記オブジェクトをローカルに保存した場合にローカルに保存された前記特定の電子情報から前記オブジェクトを利用可能なように前記特定の電子情報を変更し、変更された前記特定の電子情報をコピーされた前記オブジェクトと共に記憶装置に格納する第 2 ステップと、

コピーされた前記特定の電子情報と、コピーされた前記オブジェクトと、変更された前記特定の電子情報と、前記ネットワーク上における前記特定の電子情報の所在に関する情報を含む属性情報とを日時と共にユニークに特定し且つ認証する電子証明書を取得する第 3 ステップと、

変更された前記特定の電子情報に対応して、前記電子証明書及び前記属性情報を記憶装置に格納する第 4 ステップと、

を実行させるためのプログラムを格納した記憶媒体。

【請求項 1 4】 ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明するためのプログラムを格納した記憶

媒体であって、

前記プログラムは、前記特定のコンピュータ以外のコンピュータに、

記録依頼に応じて、前記特定のコンピュータに格納された前記特定の電子情報にアクセスし、前記特定の電子情報及び当該特定の電子情報が第 2 の電子情報又はオブジェクトを参照している場合には当該第 2 の電子情報又はオブジェクトをコピーする第 1 ステップと、

前記特定の電子情報及び前記第 2 の電子情報又はオブジェクトをローカルに保存した場合にローカルに保存された前記特定の電子情報から前記第 2 の電子情報又はオブジェクトを利用可能なように前記特定の電子情報を変更し、変更された前記特定の電子情報をコピーされた前記第 2 の電子情報又はオブジェクトと共に記憶装置に格納する第 2 ステップと、

コピーされた前記特定の電子情報及び前記第 2 の電子情報又はオブジェクトと、変更された前記特定の電子情報と、前記ネットワーク上における前記特定の電子情報の所在に関する情報を含む属性情報とを日時と共にユニークに特定し且つ認証する電子証明書を取得する第 3 ステップと、

変更された前記特定の電子情報に対応して、前記電子証明書及び前記属性情報を記憶装置に格納する第 4 ステップと、

を実行させるためのプログラムを格納した記憶媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明が属する技術分野】

本発明は、ネットワーク上の電子情報が公開されていたことを証明するための方法、システム及びコンピュータ・プログラム並びに該コンピュータ・プログラムを格納した記録媒体に関する。

【0 0 0 2】

【従来の技術】

従来から、特定の電子情報が特定の日に存在していたことを認証する方法及びシステムは存在していた。このような方法及びシステムは、例えば米国特許第 5 1 3 6 6 4 7 号、米国再審査特許第 R E 3 4 9 5 4 号、米国特許第 5 1 3 6 6

4 6 号、米国特許第 5 3 7 3 5 6 1 号、米国特許第 5 7 8 1 6 2 9 号などに記載されている。しかし上で述べた米国特許の技術は、例えばインターネット等で、特定の電子情報が公開されていたことを証明するものではない。

【0 0 0 3】

【発明が解決しようとする課題】

近年、インターネット等でも技術情報が開示されるようになり、このような技術情報は、雑誌や図書等の形で刊行された技術情報と同等の内容の情報を含んでおり、その伝達の迅速性等は従来の刊行物とは比較にならないほどである。よって、研究者が自己の研究成果を早期に公表すること等を目的としてインターネット等を使用することも多くなっている。また、従来の刊行物に比して情報の発信が簡便であり、コストも低いため、より多くの情報がインターネット等で公開される可能性が高い。しかし、従来技術では電子情報が存在していたことを証明することはできるが、インターネット等で公開されていたということを証明することはできなかった。

斯かる場合、即ちインターネット等で公開されていたということを証明することができない場合には、公開されていた技術内容と同様の内容の特許を他人が取得してしまうという恐れがある。上述の通り、インターネット等で公開された技術情報は、実質的に刊行物と同じ効果を奏するものであり、日本においては「電子通信回線を通じて公衆に利用可能になった発明」に対しては特許を与えないような法律が制定されている。しかし、インターネット等で公開された技術情報は、いつ公開されていたのか、改ざんされていないのか、という事実を証明することが困難であるため、証拠としての信頼性が従来の刊行物に比して弱い、という面は否めない。

さらに、インターネット等で使用されている HTML (Hyper Text Markup Language) 等による文書には、様々なオブジェクトが、インラインで埋め込まれている場合もある。このオブジェクトは、静止画像、動画像、サウンド、Java アプレット (Java は Sun Microsystems 社の商標) の他、ブラウザのプラグイン・ソフトウェアや補助アプリケーションを必要とするもの等もある。インターネット等で公開されている電子情報は、この HTML 等による文書と、埋め込まれて

いるオブジェクトとで構成されており、これらの組み合わせにて公衆に情報が伝達される。また、HTML等による文書にハイパーリンクが設けられ、外部リソースとして、他のHTML等による文書を含むオブジェクトが参照できるようになっているものもある。

しかし、インターネット等で公開される電子情報はオンラインで電子情報を閲覧することを前提に構成されており、その電子情報をローカルに保存した場合に、埋め込まれた又は参照されたオブジェクトがその電子情報から利用可能となっていない場合が多い。これでは、電子情報全体がどのような情報をネットワーク上で公開していたかを、ネットワークで公開しなくなった後に示すことができない。

そこで、本発明は、インターネット等のネットワーク上で、特定の電子情報が所定の条件の下公開されていたこと及び特定の電子情報のオンラインにおける情報伝達状態を証明するための方法、システム及び並びに該コンピュータ・プログラムを格納した記録媒体を提供することを目的とする。

【0004】

【課題を解決するための手段】

本発明の第1の態様に係る、ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明する方法は、記録依頼に応じて、特定のコンピュータに格納された当該特定の電子情報にアクセスし、特定の電子情報及び当該特定の電子情報にオブジェクトが含まれる場合には当該オブジェクトをコピーする第1ステップと、特定の電子情報及びオブジェクトをローカルに保存した場合にローカルに保存された当該特定の電子情報からオブジェクトを利用可能なように特定の電子情報を変更し、変更された特定の電子情報をコピーされたオブジェクトと共に記憶装置に格納する第2ステップと、コピーされた特定の電子情報及びオブジェクトと、変更された特定の電子情報と、ネットワーク上における特定の電子情報の所在に関する情報を含む属性情報とを日時と共にユニークに特定し且つ認証する電子証明書を取得する第3ステップと、変更された特定の電子情報に対応して、電子証明書及び属性情報を記憶装置に格納する第4ステップとを含む。このようにすると、ネットワーク上で公開されていた電子

情報そのものと、オンラインにおける情報伝達状態を擬似的に再現できるようにした電子情報、即ち上で述べた「変更された特定の電子情報」との両方の証明書を取得できるので、電子情報全体で実質的にどのような情報がネットワークを介して公開されていたのかを後日証明することができるようになる。

なお、コピーされた当該特定の電子情報を記憶装置に格納する第 5 ステップをさらに含むようにすることも可能である。

また、証明依頼等に応じて、記憶装置に格納された、電子証明書と属性情報と変更された電子情報とオブジェクトとを当該証明依頼元に提供する第 6 ステップをさらに含むようにすることも可能である。

さらに、特定の電子情報から参照される第 2 の電子情報又は第 2 のオブジェクトにアクセスし、第 2 の電子情報又は第 2 のオブジェクトをコピーする第 7 ステップをさらに含み、上で述べた第 2 ステップを、特定の電子情報及びオブジェクト並びに第 2 の電子情報又は第 2 のオブジェクトをローカルに保存した場合にローカルに保存された特定の電子情報からオブジェクト並びに第 2 の電子情報又は第 2 のオブジェクトを利用可能なように特定の電子情報を変更するステップを含むように構成し、上で述べた第 3 ステップを、コピーされた特定の電子情報及びオブジェクト並びに第 2 の電子情報又は第 2 のオブジェクトと、変更された特定の電子情報と、ネットワーク上における特定の電子情報の所在に関する情報を含む属性情報とを日時と共にユニークに特定し且つ認証する電子証明書を取得するステップとすることも可能である。これにより特定の電子情報のリンク先のオブジェクト等についても、証明対象とすることができる。

なお、上で述べたネットワークにはインターネットが最も適用し易く、その場合、電子情報は HTML (Hyper Text Markup Language)、XML (eXtensible Markup Language) 等のマークアップ・ランゲージにより記述された電子文書であり、ネットワーク上における電子情報の所在に関する情報はユニフォーム・リソース・ロケータ (URL) であり、アクセス条件は、少なくともアクセス元の IP アドレスを含むとすることが可能である。さらに、電子情報に含まれるオブジェクトは、静止画像、動画像、サウンド、アプレット、又は電子情報により指定されたフォーマットのデータとし得る。

【0 0 0 5】

本発明の第 2 の態様に係る電子情報公開証明方法は、記録依頼に応じて、特定のコンピュータに格納された特定の電子情報にアクセスし、特定の電子情報及び当該特定の電子情報が第 2 の電子情報又はオブジェクトを参照している場合には当該第 2 の電子情報又はオブジェクトをコピーする第 1 ステップと、特定の電子情報及び第 2 の電子情報又はオブジェクトをローカルに保存した場合にローカルに保存された当該特定の電子情報から第 2 の電子情報又はオブジェクトを利用可能なように当該特定の電子情報を変更し、変更された特定の電子情報をコピーされた第 2 の電子情報又はオブジェクトと共に記憶装置に格納する第 2 ステップと、コピーされた特定の電子情報及び第 2 の電子情報又はオブジェクトと、変更された特定の電子情報と、ネットワーク上における特定の電子情報の所在に関する情報を含む属性情報とを日時と共にユニークに特定し且つ認証する電子証明書を取得する第 3 ステップと、変更された特定の電子情報に対応して、電子証明書及び属性情報を記憶装置に格納する第 4 ステップとを含む。これにより、例えば電子情報とリンク先の第 2 電子情報又はオブジェクトとの関係を、後に再現できるようになる。

本発明の第 3 の態様に係る、ネットワークに接続された特定のコンピュータにおいて特定の電子情報が公開されていたことを証明するシステムは、記録依頼に応じて、特定のコンピュータに格納された当該特定の電子情報にアクセスし、特定の電子情報及び当該特定の電子情報に含まれるオブジェクトをコピーするアクセス手段と、特定の電子情報及びオブジェクトをローカルに保存した場合にローカルに保存された特定の電子情報からオブジェクトを利用可能なように特定の電子情報を変更し、変更された特定の電子情報をコピーされた前記オブジェクトと共に記憶装置に格納する変更手段と、コピーされた特定の電子情報と、コピーされたオブジェクトと、変更された特定の電子情報と、ネットワーク上における特定の電子情報の所在に関する情報を含む属性情報とを日時と共にユニークに特定し且つ認証する電子証明書を取得し、変更された特定の電子情報に対応して、電子証明書及び属性情報を記憶装置に格納する電子証明書取得手段と、記憶装置に格納された電子証明書と、属性情報と、変更された電子情報と、オブジェクトと

を証明依頼元に提供する手段とを有する。

本発明の第 3 の態様においては、電子証明書を発行する手段をさらに有する構成も可能である。

なお、本発明の第 1 の態様について説明した第 1 の態様の変更を、第 3 の態様に係る電子情報公開証明システムに対して応用可能である。

【 0 0 0 6 】

本発明の第 4 の態様に係る電子情報公開証明システムは、記録依頼に応じて、特定のコンピュータに格納された特定の電子情報にアクセスし、特定の電子情報及び当該特定の電子情報が第 2 の電子情報又はオブジェクトを参照している場合には当該第 2 の電子情報又はオブジェクトをコピーする手段と、特定の電子情報及び第 2 の電子情報又はオブジェクトをローカルに保存した場合にローカルに保存された特定の電子情報から第 2 の電子情報又はオブジェクトを利用可能なように当該特定の電子情報を変更し、変更された特定の電子情報をコピーされた第 2 の電子情報又はオブジェクトと共に記憶装置に格納する手段と、コピーされた特定の電子情報及び第 2 の電子情報又はオブジェクトと、変更された特定の電子情報と、ネットワーク上における特定の電子情報の所在に関する情報を含む属性情報とを日時と共にユニークに特定し且つ認証する電子証明書を取得し、変更された特定の電子情報に対応して、電子証明書及び属性情報を記憶装置に格納する手段と、記憶装置に格納された電子証明書と、属性情報と、変更された電子情報と、第 2 の電子情報又はオブジェクトとを証明依頼元に提供する手段とを有する。

さらに、本発明の第 1 及び第 2 の態様に係る電子情報公開証明方法をコンピュータで実行するためのプログラムとして実装することが可能であり、このプログラムは、例えばフロッピー・ディスク、CD-ROM、光磁気ディスク、半導体メモリ、ハードディスク等の記憶媒体又は記憶装置に格納される。

【 0 0 0 7 】

【発明の実施の形態】

まず、本発明の前提に係わる提供されるサービスの概略を説明しておく。例えば、依頼人 A は、(1) インターネットに接続された自己の WWW (World Wide Web) サーバに格納された Web ページ (ウェブページ) が、インターネット上

で相当期間公開されていることを記録すること、及び（２）W e b ページの存在及びその存在場所を公衆が知り得るようにするため当該W e b ページにリンクを貼ることを、本サービスの提供者Bに依頼する、とする。

本依頼を受けたサービス提供者Bは、依頼人Aの知らない任意のタイミングで、指定されたU R L のW e b ページに、依頼人Aの知らないI P アドレスからアクセスし、当該W e b ページをコピーする。次に、サービス提供者Bは、W e b ページのU R L 及びアクセス元のI P （Internet Protocol）アドレス等を含む属性情報を生成し、W e b ページのコピー及びその属性情報を、日時と共にユニークに特定し且つ認証する電子証明書を取得する。そして、サービス提供者Bは、W e b ページのコピー及び属性情報と、取得した電子証明書とを対応付けて保存する。

サービス提供者Bは、依頼人Aの知らない任意のタイミングで、再度指定されたU R L のW e b ページにアクセスし、当該W e b ページをコピーする。この際、アクセス元のI P アドレスを変更してアクセスすることにより、依頼人AのW W Wサーバがアクセス制限をしていないという証明を付加的に得ることができる。次に、サービス提供者Bは、上と同じように属性情報を生成し、W e b ページのコピー及びその属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得する。そして、サービス提供者Bは、W e b ページのコピー及び属性情報と、取得した電子証明書とを対応付けて保存する。サービス提供者Bは、このような処理を依頼人Aの指定した相当期間繰り返す。

また、サービス提供者Bは、（２）の依頼に対し、指定されたW e b ページのU R L へのリンクをインターネットに接続された自己のW W WサーバのW e b ページに掲載し、一般公衆がアクセス可能にする。例えば、当該リンクを、依頼人ごと、又は内容の分野毎に検索できるようにしておく場合もある。なお、W W Wサーバにリンクを掲載していたことについても掲載期間等と共に記録を残しておく。

【 0 0 0 8 】

依頼人Aは、上の依頼と同時に又は必要となった時に、上の（１）で指定したW e b ページに対する記録内容の提供をサービス提供者Bに申し込むことができ

る。この申込みに対応してサービス提供者Bは、保存したW e b ページのコピーと属性情報と電子証明書とを依頼人Aに提供する。この際、例えばC D - R 等の上で述べたデータを書き込んで提供することも可能であるし、インターネットを介して提供することも可能である。さらに、上の（２）の結果として、サービス提供者BのWWWサーバに、指定したW e b ページへのリンクが掲載されていたこと及びその期間等についての記録を証明書として、依頼人Aに提供する場合もある。

依頼人Aは、サービス提供者Bから提供を受けた情報を当該W e b ページがインターネット上で相当期間公開していたことの証明として使用できる。

依頼人Aは、上で述べた（１）及び（２）の他に、（３）インターネット上の一般公衆向け検索エンジンで、指定したW e b ページが検索できるということの記録をサービス提供者Bに依頼することもできる。これは、W e b ページの存在及び存在場所を公衆がより知り易い状態にあったことの証拠となる。サービス提供者Bは、任意の検索エンジンで、適切なキーワード等で検索を行う。指定されたW e b ページが検索できた場合には、当該検索できたという事実及び使用した検索エンジンのアドレス及び名称、並びに使用したキーワード、検索日時等を記録する。この記録を証明書として、記録内容提供依頼に応じて、依頼人Aに提供する場合もある。

【 0 0 0 9 】

依頼人Aは、（１）では自己のWWWサーバに格納されたW e b ページについて記録することを依頼していたが、（１）'他人のWWWサーバに格納されたW e b ページについて記録することをサービス提供者Bに依頼できる。この場合、サービス提供者Bは上の（１）で述べたような処理を同じように実施する。しかし、他人のWWWサーバのW e b ページが、依頼人Aの指定した相当期間中存在し続ける保証は無く、存在しなくなってしまうたり、改変される場合もある。存在しなくなってしまう場合には、サービス提供者Bは、インターネット上で公開が確認された期間を記録し、依頼人Aの記録内容提供依頼に応じて、通常提供する情報に加え当該期間を提供する場合もある。改変される場合には、上で述べた処理を実施すれば、改変の履歴が残る。なお、他人のWWWサーバに格納され

たW e b ページは、依頼人AがそのU R Lを指定してもよいし、例えば指定された検索エンジンで指定されたキーワード検索を行った結果の全てのU R Lといった指定も可能である。

また、依頼人Aは、(4) 自己又は他人のWWWサーバに格納されたW e b ページのバージョン遷移の記録をサービス提供者Bに依頼することもできる。サービス提供者Bは、例えば、(1)と同じ処理を実施する。但し、サービス提供者Bは、前回アクセスした時のW e b ページの内容と、今回アクセスした時のW e b ページの内容とが異なるかを検査する。異なる場合には、例えば、以前と異なっていたということを記録する。

なお、サービス提供者BがW e b ページのコピーを保存する必要は無い。例えば依頼人Aが保存すれば良い。サービス提供者BがW e b ページのコピーを保存しない場合には、(1)及び(1)'の処理でアクセス毎に保存されるのは、属性情報と電子証明書だけである。また、(4)の場合、前回アクセスした時のW e b ページの内容と今回アクセスした時のW e b ページの内容が異なっていた場合、その差分を保存する又は異なっていた場合にのみW e b ページ全体を保存する等により、バージョンの変更を保存することができる。

また(1)及び(1)'の記録依頼における記録期間、回数、頻度等は、依頼人Aにより指定できる。サービス提供者Bはそれに従って記録を行う。

さらに、(2)乃至(4)のサービスはオプションとすることができ、特に(2)及び(3)といったサービスは、他の媒体等でW e b ページの存在及び所在が公衆に明らかになっていれば必要ない。

【0 0 1 0】

一方サービス提供者Bは、本サービスを続けていくと、インターネットを介して公開されていたという電子証明書付きのW e b ページを多数保持することになる。この情報を用いて、サービス提供者Bは、(5) 電子証明書付きのW e b ページ提供サービスを行うことができる。例えば、サービス提供者Bは、インターネットを介してキーワード検索等ができるようなデータベースを構築し、第3者に検索サービスを提供する。そして検索者Sの記録内容提供依頼に応じて、インターネットを介して又はC D - Rのような媒体で、記録内容を提供する。また、

電子証明書付きの Web ページの要約を作成し、その要約で検索のスクリーニングができるような形態にデータベースを構築する場合もある。

以上のようなサービスを提供するための電子情報公開証明システムの概要を図 1 に示す。ネットワーク 1 には、3 で示すサーバ A、5 で示すサーバサーバ B、7 で示すサーバ C、9 で示すサーバ D、1 1 で示すサーバ E 及び図示されない多数のコンピュータが接続されている。ネットワーク 1 は例えばインターネットである。3 で示すサーバ A は、WWWサーバであり、電子情報、例えば URL が `http://www.abcd.co.jp` である Web ページ 3 1 を格納しており、ネットワーク 1 で公開している。

5 で示すサーバ B は、サービス提供者が管理するサーバであり、依頼人指定の電子情報にアクセスし、コピーを取得するコピー取得機能 5 1 と、例えば URL 等の電子情報の所在に関する情報及びアクセス条件を含む属性情報を生成する属性情報生成機能 5 3 と、電子情報のコピー及び属性情報を日時と共にユニークに特定し且つ認証する電子証明書を取得する証明書取得機能 5 5 と、必要な情報を保存する保存機能 5 7 と、依頼人の申し出に対応して保存されている電子証明書等を提供するための証明書提供機能 5 9 とを含む。この 5 で示すサーバ B には記憶装置 6 1 が接続されている。

7 で示すサーバ C は、特定の電子情報を日時と共にユニークに特定し且つ認証する証明書を発行するタイムスタンプ証明書発行機能 7 1 を有している。7 で示すサーバ C は、ネットワーク 1 を介して証明書発行依頼を受け取り、タイムスタンプ証明書発行機能 7 1 にて電子証明書を発行し、依頼元に電子証明書を送り返す。

【 0 0 1 1 】

9 で示すサーバ D は、5 で示すサーバ B に機能を付加するためのサーバであって、例えば WWWサーバとして依頼人が指定した Web ページへのリンク 9 1 を掲載する。但し、このようなリンク 9 1 のデータベースを作成し、リンク先 Web ページの内容又は所有者等毎に検索可能にしておく場合もある。さらに、5 で示すサーバ B に接続されている記憶装置 6 1 のデータを用いてデータベース 9 5 を作成し、9 で示すサーバ D がこのデータベース 9 5 をネットワークを介して検

索可能にする検索機能 9 3 を保持している場合もある。さらに、記憶装置 6 1 のデータから各電子情報の要約を作成し、この要約に関するデータベース 9 7 を検索機能 9 3 がネットワークを介して検索可能にする場合もある。

1 1 で示すサーバ E は、一般公衆向け検索エンジンである。この一般公衆向け検索エンジンは、従来と変わらないので説明は割愛する。

次に、本発明により提供されるサービス (1) 及び (1) ' を、図 1 に示したシステムの動作として説明する。

依頼者 A は例えば 3 で示すサーバ A の URL `http://www.abcd.co.jp` の Web ページを相当期間記録すべき電子情報として指定し、サービス (1) 又は (1) ' をサービス提供者 B に依頼する。サービス提供者 B は 5 で示すサーバ B を用いて処理を行う。5 で示すサーバ B のコピー取得機能 5 1 は、任意のタイミングで `http://www.abcd.co.jp` に例えばルート (A) によりアクセスし、Web ページ 3 1 のコピーを例えばルート (B) を介して取得する。コピーは、例えば 5 で示すサーバ B のメインメモリに保持される。コピー取得機能 5 1 は、アクセス毎に、アクセス元の IP アドレスを記憶装置に記憶しておく。コピー取得機能 5 1 は、アクセス条件を決定する機能を含んでおり、例えば依頼人が指定した相当期間中、どのタイミングで且つどのアクセス元 IP アドレスを使用してアクセスするか決定する。また、依頼人が頻度を指定している場合には、当該頻度の指定を満たすように、アクセスをスケジューリングする。

属性情報生成機能 5 3 は、このアクセス元の IP アドレスと依頼人 A 指定の URL とを含む属性情報を生成する。属性情報には、IP アドレス及び URL のほかに、例えば 5 で示すサーバ B が図示しないプロキシ・サーバを介してネットワーク 1 に接続している場合には、このプロキシ・サーバの IP アドレスや、アクセス日時を含むようにしてもよい。

【 0 0 1 2 】

証明書取得機能 5 5 は、取得した Web ページ 3 1 のコピー及び生成した属性情報に対して電子証明書を取得する。より具体的な処理については後に詳述する。図 1 のシステムでは、証明書取得機能 5 5 は、ネットワーク 1 の例えばルート (C) を介して発せられる電子証明書発行依頼を、7 で示すサーバ C のタイムス

タイムスタンプ証明書発行機能 7 1 にて受領し、タイムスタンプ証明書機能 7 1 により発行される電子証明書をネットワーク 1 の例えばルート (D) を介して受領する。タイムスタンプ証明書発行機能 7 1 については後に詳しく述べるものとする。

保存機能 5 7 は、コピー取得機能 5 1 が取得した Web ページ 3 1 のコピーと、属性情報生成機能 5 3 が生成した属性情報と、証明書取得機能 5 5 が取得した電子証明書とを、記憶装置 6 1 に格納する。但し、コピー取得機能 5 1 が取得した Web ページ 3 1 のコピーを保存することは任意である。例えば、依頼人 A が自分で保存する場合もあるからである。また、保存機能 5 7 は、前回コピーした Web ページ 3 1 の内容と、今回アクセスした Web ページ 3 1 の内容が同一である場合、今回取得した Web ページ 3 1 のコピーを保存しないといった判断を行うようにしてもよい。また、保存機能 5 7 は、後に証明書提供機能 5 9 が必要なデータを取り出し易いように、依頼人毎又は指定された URL 等毎にデータを保存しておく。

記録依頼と同時に又は任意のタイミングで依頼人 A は記録内容の提供を申し出る。この際、証明書提供機能 5 9 は、それに応じて、依頼の対象となる Web ページ 3 1 のコピー、属性情報及び電子証明書を記憶装置 6 1 から読み出し、図 1 の例では CD-R 6 3 等の記憶媒体に格納して、依頼人 A に提供する。なお、Web ページ 3 1 のコピー、属性情報及び電子証明書は、アクセス毎に記憶されるが、証明書提供機能 5 9 はこれらを全て CD-R 等の記憶媒体に格納して提供してもよいし、Web ページ 3 1 のコピーに変化がない場合には、最初のアクセス時の Web ページ 3 1 のコピーと全ての属性情報及び全ての電子証明書を提供するようにしてもよい。さらに、証明書提供機能 5 9 において、属性情報及び電子証明書を用いて、URL、アクセス元 IP アドレス及び証明書日時を含むアクセス記録を作成し、当該アクセス記録と、最初のアクセス時の Web ページ 3 1 と、全ての属性情報と、全ての電子証明書とをサービス提供者 B による証明書として提供するようにすることも可能である。なお、保存機能 5 7 が Web ページ 3 1 のコピーを保存しない場合には、当然証明書提供機能 5 9 も依頼人 A に Web ページ 3 1 のコピーを提供しない。

【0013】

次に、本発明により提供されるサービス（２）を、図 1 に示したシステムに基づき説明する。（２）は、W e b ページの存在及びその存在場所を公衆が知り得るようにするため当該W e b ページにリンクを貼ることを、依頼人 A がサービス提供者 B に依頼するものである。

この依頼に応じてサービス提供者 B は、ネットワーク 1 に接続された 9 で示すサーバ D に、3 で示すサーバ A に格納されたW e b ページ 3 1 へのリンク 9 1 を掲載する。依頼数が少なければ、9 で示すサーバ D に格納されたW e b ページに、単に指定されたW e b ページのU R L を掲載するだけでも良い。しかし、依頼数が多い場合には、リンクについてのデータベースを構築し、ネットワーク 1 を介して、第三者が、W e b ページの内容又は依頼人の業種等によって検索できるようにする場合もある。サービス提供者 B は、W e b ページ 3 1 へのリンク 9 1 を自己のW e b ページに掲載していた期間や、検索可能であった期間を記憶装置に記録しておき、後に依頼人 A 等から求められた時には、当該記録を証明書として提供する。

次に、本発明により提供されるサービス（３）を、図 1 に示したシステムに基づき説明する。（３）は、ネットワーク 1 上の一般公衆向け検索エンジンである 1 1 で示すサーバ E で、指定したW e b ページが検索できるということの記録をサービス提供者 B に依頼をするものである。

サービス提供者 B は、例えば 5 で示すサーバ B を介して、1 1 で示すサーバ E における検索エンジンで、適切なキーワード等により検索を行い、指定されたW e b ページ 3 1 が検索できた場合には、当該検索できたという事実及び 1 1 で示すサーバ E の名称及びアドレス、使用したキーワード、検索日時等を記憶装置に記録する。後に依頼人 A 等から求められた時には、この記録を証明書として提供する。

【 0 0 1 4 】

次に、本発明により提供されるサービス（４）を、図 1 に示したシステムに基づいて説明する。（４）は、W e b ページ 3 1 のバージョン遷移の記録をサービス提供者 B に依頼するものである。

サービス提供者 B は、5 で示すサーバ B を用いて（１）と同様な処理を行う。

すなわち、所定のタイミングで 3 で示すサーバ A の W e b ページ 3 1 にアクセスし、W e b ページ 3 1 のコピーを取得する。次に、U R L 及びアクセス条件を含む属性情報を生成し、属性情報及び W e b ページ 3 1 のコピーに対し電子証明書を取得する。そして、少なくとも属性情報及び電子証明書を記憶装置 6 1 に保存する。W e b ページ 3 1 のコピーを記憶装置に保存するようにすることも可能である。次に、所定のタイミングにて 3 で示すサーバ A の W e b ページ 3 1 にアクセスし、同様な処理を行い、属性情報及び W e b ページ 3 1 のコピーに対し電子証明書を取得する。そして、前回アクセスした時の W e b ページ 3 1、より正確には、最も最近変更が検出された時の W e b ページ 3 1、の内容と、今回アクセスした時の W e b ページ 3 1 の内容が異なっているか判断する。この判断を、コピー取得機能 5 1 が行っても、保存機能 5 7 が行ってもかまわない。内容が異なっている場合には、少なくとも属性情報及び電子証明書に加え、異なっていたということを記憶装置に記録する。場合によっては、前回アクセスした時の W e b ページ 3 1 の内容と今回アクセスした時の W e b ページ 3 1 の内容の差分を記憶装置に記録するようにしてもよいし、異なっている場合には、必ず W e b ページ 3 1 の全体のコピーを記憶装置に保存するようにしてもよい。

依頼人 A 等から求められたときには、サービス提供者 B は、証明書提供機能 5 9 により、少なくとも属性情報及び電子証明書と変更の有無の記録を提供する。差分や異なる毎に W e b ページ全体を提供してもよい。

【 0 0 1 5 】

次に、本発明により提供されるサービス (5) を、図 1 に示したシステムに基づき説明する。(5) は、電子証明書付きの W e b ページ提供サービスである。

サービス提供者 B は、9 で示すサーバ D に検索機能 9 3 を設け、記憶装置 6 1 に蓄えられた電子証明書及び属性情報付きの W e b ページ 3 1 のコピーを使用して、データベース 9 5 を作成する。そして、第三者に検索機能 9 3 からデータベース 9 5 を検索できるようにする。第三者が使用を欲する W e b ページ 3 1 のコピーを見つけた場合には、ネットワーク 1 等を介して、記録内容提供依頼をサービス提供者 B に提出する。サービス提供者 B は、証明書提供機能 5 9 を使用して、例えば C D - R 6 3 等に提供を求められた W e b ページ 3 1 のコピー及び属性

情報並びに電子証明書を格納し、当該 C D - R 6 3 等を提供する。ネットワーク 1 を介して上述のようなデータを送信するようにしてもよい。

さらに、サービス提供者 B は、W e b ページ 3 1 のコピーからその要約を作成し、要約のデータベース 9 7 を構築し、検索機能 9 3 により第三者が検索可能にすることも可能である。第三者は、要約のデータベースでスクリーニングをしたのちに、W e b ページ 3 1 のコピーを確認し、必要な電子情報の記録内容提供依頼を出すことができるようになる。

本発明の主要なサービス (1) 及び (1) ' の処理フローを図 2 にまとめた。依頼人 A から、例えば W e b ページ等の記録対象電子情報に関する、例えば U R L 等の所在に関する情報及び例えば記録期間等の記録条件を指定した記録依頼がサービス提供者 B に出された場合 (ステップ S 1) には、記録条件に合致するようにコピー取得機能 5 1 は、アクセス条件を決定 (ステップ S 3) し、当該 U R L に所定のタイミングで所定のアクセス元 I P アドレスからアクセスして、W e b ページのコピーを取得 (ステップ S 5) する。そして、属性情報生成機能 5 3 は、W e b ページの U R L とアクセスの条件としてアクセス元 I P アドレスとを含む属性情報を生成 (ステップ S 7) する。

その後、証明書取得機能 5 5 は、属性情報及び取得した W e b ページのコピーを日時と共に特定し且つ認証する電子証明書を、タイムスタンプ証明書発行機能 7 1 から取得 (ステップ S 9) する。なお、5 で示すサーバ B が、タイムスタンプ証明書発行機能 7 1 を含むような構成とすることも可能であって、その場合証明書取得機能 5 5 はタイムスタンプ証明書発行機能 7 1 に置き換えられる。

そして、保存機能 5 7 は、少なくとも属性情報及び電子証明書を記憶装置 6 1 に格納 (ステップ S 1 1) する。なお、上でも述べたが、W e b ページのコピーを記憶装置に保存するかは任意である。そして、この処理を記録終了の条件が満たされるまで繰り返す (ステップ S 1 3) 。記録終了の条件とは、例えば依頼人 A の指定した記録期間が終了した場合や、依頼人 A の指定した記録回数に達した場合等である。

【 0 0 1 6 】

次に依頼人 A による記録内容提供依頼に応じて実行される処理フローの例を図

3に示す。記録内容提供依頼（ステップS 4 1）には対象となる電子情報が含まれているので、まず証明書提供機能5 9は、対象となる電子情報を特定（ステップS 4 3）する。そして、証明書提供機能5 9は、記憶装置6 1から対象電子情報のコピーと、電子証明書及び属性情報を読み出す（ステップS 4 5）。なお、記録依頼が1回だけの記録を要求していたり、結果的に1回アクセスしただけで対象電子情報が無くなったりする場合には、読み出されるデータは1セットのみであるが、通常複数回に渡って記録しているので、電子情報のコピーと属性情報と電子証明書のセットを複数読み出すことになる。

そして、証明書提供機能5 9は、公開期間の計算を付加的に行う（ステップS 4 7）。電子証明書には日時の記録が含まれるので、初回アクセス時に取得した電子証明書と最後にアクセスした時に取得した電子証明書とを参照すれば、少なくともいつからいつまで公開されていたか分かるので、この情報を公開期間とする。但し、この処理は任意である。

最後に、証明書提供機能5 9は、対象電子情報のコピーと、電子証明書及び属性情報、並びに公開期間情報を、例えばC D - R等の媒体に格納して提供（ステップS 4 9）することで終了（ステップS 5 1）する。

ここで電子証明書について図4を用いて簡単に説明しておく。本発明では、電子情報を日時と共にユニークに特定し且つ認証する電子証明書を発行するものであれば、どのような方式にて電子証明書を発行してもよい。よって、以下の説明は一例であって、他の方式にて電子証明書を発行することにしてもよい。

電子情報1 0 1を電子証明書の対象であるとする、まず、電子情報1 0 1に対してハッシュ値1 0 3を計算する。ハッシュ関数は一方向関数であれば何でも良い。ハッシュ値の計算までを例えば証明書取得機能5 5が行う。そして、このハッシュ値1 0 3を含む証明書発行依頼を、タイムスタンプ証明書発行機能7 1に送る。タイムスタンプ証明書発行機能7 1は、同じように送られてきた他のハッシュ値と共に処理をする。例えば図4のように、2つのハッシュ値からもう一つのハッシュ値を生成するといった処理を繰り返し、送られてきた全ハッシュ値から最終的に一つのハッシュ値1 0 6を生成する。このハッシュ値1 0 6と、時刻T - 1（Tは整数）におけるSHV（Super Hash Value:スーパー・ハッシュ

値) 1 0 5 とを用いて時刻 T における S H V 1 0 7 を生成する。このようにして生成された時刻 T における S H V 1 0 7 とハッシュ値 1 0 3 と、時刻 T の時刻情報と、文書 I D とが電子証明書 1 0 9 を構成する。この電子証明書 1 0 9 はハッシュ値 1 0 3 の送り主に送信され、電子情報 1 0 1 と電子証明書 1 0 9 とを対にして、電子情報 1 0 1 を日時と共にユニークに特定し且つ認証することができるようになる。

【0 0 1 7】

なお、W e b ページを図 4 の電子情報とする場合には、H T M L 文書が電子情報に当たる。但し、W e b ページの内容が文章だけであればよいが、通常 W e b ページには例えば G I F ファイル等の画像ファイル等が埋め込まれている。例えば図 5 で示したように、3 で示すサーバ A の W e b ページ 3 1 をネットワーク 1 に接続した図示しないクライアント・コンピュータのブラウザで見たときには、静止画像等のオブジェクト 2 0 1 及び 2 0 3 がインラインで埋め込まれている W e b ページ 2 0 0 のように表示される。W e b ページに埋め込まれているのは、静止画像のみならず、動画像であったり、サウンドであったり、ブラウザのプラグイン等を必要とするフォーマットのファイルであったり、J a v a (Sun Microsystems 社の商標) アプレットであったりする。このような場合には、W e b ページに埋め込まれたオブジェクトの内容もネットワーク上で公開されていた情報に含まれる。

さらに、例えば図 5 では外部リソースということで、W e b ページ 2 0 0 には、他の W e b ページ又はオブジェクトへのリンク 2 0 5 乃至 2 0 9 が含まれている。このリンク先の W e b ページ又はオブジェクトは、この W e b ページの U R L で公開されている内容とは言えないが、ネットワーク 1 の利用者は簡単にリンク先の電子情報を得ることができる。よって、これらの電子情報についても公衆利用可能性があると言える。また、リンク 2 0 5 乃至 2 0 9 先の W e b ページ又はオブジェクトは、W e b ページ 2 0 0 と関連性がある場合が多く、W e b ページ 2 0 0 の H T M L 文書を作成した者は、W e b ページ 2 0 0 及びリンク先の W e b ページ又はオブジェクトによる一体とした情報の開示を意図している場合もある。よって、このリンク先の W e b ページ又はオブジェクトを電子証明書取得

の対象にするか否かという問題も生ずる。

加えて、例えば図 5 に示した W e b ページ 2 0 0 の H T M L 文書及びオブジェクト 2 0 1 及び 2 0 3 をそれぞれファイルとして例えば 5 で示すサーバ B にローカルに保存し、そのローカルに保存した H T M L 文書をブラウザで見てみる。そうすると、図 6 に示したように、W e b ページ 2 0 0 a には、前記したオブジェクト 2 0 1 及び 2 0 3 の枠 2 0 1 a 及び 2 0 3 a のみが表示される。場合によっては、読み込まれなかったことを示すマーク 2 0 1 b 及び 2 0 3 b が枠内に表示される。さらに、リンク 2 0 5 乃至 2 0 9 をポインタにて選択しても、リンク先の W e b ページ又はオブジェクトを見ることはできない。

【 0 0 1 8 】

これは、例えば W e b ページ 2 0 0 の H T M L 文書に以下のような H T M L による記述があるからである。表 1 はインラインでオブジェクトが埋め込まれる場合を示している。表 2 は、リンクにて外部リソースを利用する場合である。

【表 1】

```
<IMG SRC="/image/image01.gif">  
<OBJECT DATA="/video/video.avi" TYPE="video/avi"></OBJECT>  
<APPLET CODE="/applet/animator.class" WIDTH=100 HEIGHT=100></APPLET>
```

【表 2】

```
<A HREF="/image/image02.gif">1. 画像</A>  
<A HREF="http://www.xyza.co.jp/home.html">2. W e b ページ</A>
```

例えば表 1 の第 1 行目は、W e b ページ 2 0 0 の H T M L 文書が存在するディレクトリの下に image というディレクトリがあり、その中の G I F ファイル image 01.gif を表示することを意味している。当然、W e b ページ 2 0 0 の H T M L 文書を 5 で示すサーバ B のローカルに保存した場合には、その H T M L 文書を保存したディレクトリの下に image というディレクトリが存在していることは保証されず、且つその中に image01.gif が保存されることも保証されない。

また表 1 の第 2 行目は、W e b ページ 2 0 0 の H T M L 文書が存在するディレクトリの下に video というディレクトリがあり、その中の M I M E の形式で video /avi の video.avi という動画ファイルを表示することを意味している。当然、

H T M L 文書を 5 で示すサーバ B に保存した場合には、その H T M L 文書を保存したディレクトリの下に video というディレクトリが存在していることは保証されず、且つその中に video. avi が保存されるという保証も無い。

表 1 の第 3 行目は、W e b ページ 2 0 0 の H T M L 文書が存在するディレクトリの下に applet というディレクトリがあり、その中の J a v a アプレット animat or. class が実行され、所定の表示が枠 1 0 0 × 1 0 0 の中になされるということを意味している。上と同じで、H T M L 文書を 5 で示すサーバ B に保存した場合には、その H T M L 文書を保存したディレクトリの下に applet というディレクトリが存在していることは保証されず、且つその中に applet. class が保存されるという保証も無い。

【 0 0 1 9 】

表 2 の第 1 行目は、W e b ページ 2 0 0 の H T M L 文書が存在するディレクトリの下に image というディレクトリがあり、その中の G I F ファイル image02. gif にリンクを貼ることを意味している。リンクが貼られただけであり、このファイルの内容は H T M L 文書を表示する際には表示されないもので、ファイルの内容はネットワーク 1 を介して自動的に送られてくるものではない。仮にこのファイルを 5 で示すサーバ B にローカルに保存するとしても、H T M L 文書を保存したディレクトリの下に image というディレクトリがあることは保証されず、且つその中に image02. gif が保存されることも保証されない。

表 2 の第 2 行目は、W e b ページ 2 0 0 の H T M L 文書が格納されたサーバとは別の U R L <http://www.xyz.co.jp/home.html> の W e b ページにリンクを貼ることを意味している。リンクが貼られただけであり、このファイルの内容は W e b ページ 2 0 0 の H T M L 文書を表示する際には表示されないもので、リンク先 W e b ページの H T M L 文書はネットワーク 1 を介して自動的に送られてくるものではない。仮にこの H T M L 文書を 5 で示すサーバ B にローカルに保存するとしても、その保存先はこの U R L <http://www.xyz.co.jp/home.html> ではない。

以上のように、W e b ページ 2 0 0 の H T M L 文書を例えば 5 で示すサーバ B にローカルに保存した場合、それをブラウザ等で内容を確認しようとしても、インラインで埋め込まれたオブジェクトや、リンク先の内容を見ることはできない

。これでは、HTML 文書を保存しておいても、後にネットワーク 1 で公開していた内容を正確に把握できない。

よって、本発明では、Web ページ 2 0 0 の HTML 文書のコピーの一つは原本保存のためそのまま保存し、もう一つのコピーを後に閲覧した場合にその Web ページ全体の内容を把握できるように変更する。

例えば、表 1 及び表 2 の場合には、以下のように Web ページ 2 0 0 の HTML 文書を変更する。

【表 3】

```
<IMG SRC="image01.gif">  
<OBJECT DATA="video.avi" TYPE="video/avi"></OBJECT>  
<APPLET CODE="animator.class" WIDTH=100 HEIGHT=100></APPLET>
```

【表 4】

```
<A HREF="/reference/image02.gif">1. 画像</A>  
<A HREF="/reference/home.html">2. Web ページ</A>
```

【0 0 2 0】

表 3 は、インラインで埋め込まれるオブジェクトを、変更された HTML 文書と同じディレクトリに保存することを示している。一回のアクセスで取得及び生成される、属性情報、電子証明書、Web ページ 2 0 0 の HTML 文書及び変更された HTML 文書を、これらのオブジェクトと共に同じディレクトリの下に保存する方が管理上簡単になるためである。但し、これは一例であって、5 で示すサーバ B に接続された記憶装置 6 1 にデータを記憶する場合のルールとして、インラインで埋め込まれるオブジェクトを格納するためのディレクトリを別途作成し、そのディレクトリに保存するというルールを採用する場合もある。

表 4 は、外部リソースとして参照されるオブジェクト又は他の Web ページの HTML 文書を、変更された HTML 文書を格納したディレクトリの下に reference というディレクトリに保存することを示している。このように、インラインではなく外部リソースとして参照されているオブジェクト又は他の Web ページの HTML 文書の場合には、これらを取得しないという場合もあるので、別途ディレクトリを作成して、そこに格納する。但し、これは一例であって、5 で示す

サーバBに接続された記憶装置 6 1 にデータを記憶する場合のルールとして、外部リソースとして参照されるオブジェクト又は他のWebページのHTML文書も、元のHTML文書及び変更したHTML文書と同じディレクトリに保存するというルールを採用することも可能である。

いずれにしろ、Webページがインラインでオブジェクトを含む場合、及び外部リソースとしてオブジェクト又は他のWebページを参照する場合には、原本としてWebページ200のHTML文書のファイルと、インラインで埋め込まれる又は外部リソースとして参照されるオブジェクト又はHTML文書のファイルとをそのまま保存し、閲覧用に、変更されたHTML文書を生成し且つ保存する。そして、これらのファイルと属性情報とに対し電子証明書を取得する。

よって図1に示した5で示すサーバBの構成を図7に示すの5'のようなサーバBに変形する。すなわち、コピー取得機能151は、指定された電子情報以外にも、インラインで埋め込まれたオブジェクト及び外部リソースとして参照されるオブジェクト又は他の電子情報を取得する。そして、コピー変形機能153は、上で述べたように、埋め込まれるオブジェクト又は参照先のオブジェクト又は他の電子情報の読み出し元を変更する。そして、属性情報生成機能155は、これらの電子情報及びオブジェクトに対する属性情報を生成する。この際、参照先の電子情報又はオブジェクトのコピーを取得している場合には、属性情報にその元の参照先を含める場合もある。また、どのようなファイルのコピーを電子証明書発行の対象にしているかという情報を含む場合もある。

そして、証明書取得機能157は、証明書発行対象の情報に対する電子証明書をタイムスタンプ証明書発行機能71から取得する。保存機能159は、証明書発行対象のファイルを対応するように、記憶装置61'に格納する。記憶装置61'は、電子情報のコピーと、このコピーを変形したものと、電子証明書と、オブジェクト（ここではインラインで埋め込まれている場合を想定）を格納する。証明書提供機能161は、記録内容提供依頼に応じて、記憶装置61'に格納された情報を読み出し、例えばCD-R63'を作成する。ここで、変形されたコピーと、オブジェクトとがCD-R63'に含まれているので、証明対象電子情報がオンラインで公開されていたのと同じ状態を再現できる。なお、変形前の電

子情報のコピーを保存するか及び記録内容提供依頼に応じて当該変形前の電子情報のコピーを提供するかは、任意である。

【 0 0 2 1 】

次に記録依頼に応じて行われる処理手順を図 8 を用いて説明する。依頼人 A から、例えば記録対象電子情報（例えば W e b ページ）の所在に関する情報（例えば U R L ）及び記録条件（例えば記録期間）を指定した記録依頼がサービス提供者 B に出された場合（ステップ S 6 1 ）には、記録条件に合致するようにコピー取得機能 1 5 1 は、アクセス条件を決定（ステップ S 6 3 ）し、当該 U R L に所定のタイミングで所定のアクセス元 I P アドレスからアクセスして、W e b ページのコピーを取得（ステップ S 6 5 ）する。コピー取得処理については後に詳しく述べる。記録依頼には、例えば、指定の U R L のみならず、例えばその U R L の W e b ページに含まれるリンクを 3 階層下までコピーするといった指示を含む場合もある。コピー取得機能 1 5 1 は、この指示に従ってリンク先の W e b ページ又はオブジェクトをコピーする。

次に、コピー変形機能 1 5 3 は、コピーした W e b ページがオブジェクト又はリンクを含むかを判断（ステップ S 6 7 ）する。いずれかを含む場合には、コピー変形機能 1 5 3 は、例えば上で述べたように、ローカルに保存した W e b ページのコピーにインラインで埋め込まれたオブジェクトが表示されるよう、又 W e b ページのコピーに示されているリンクを選択した場合に、リンク先の W e b ページ又はオブジェクトの内容が表示されるよう、W e b ページの H T M L 文書のコピーを変形（ステップ S 6 9 ）する。一方、W e b ページにリンクもオブジェクトも含まれない場合には、（ステップ S 7 1 ）に移行する。

そして、属性情報生成機能 1 5 5 は、W e b ページの U R L とアクセスの条件としてアクセス元 I P アドレスとを含む属性情報を生成（ステップ S 7 1 ）する。次に、証明書取得機能 1 5 7 は、W e b ページのコピー、属性情報と、インライン化されたオブジェクト又はリンクが存在する場合には、変形された W e b ページの H T M L 文書のコピーと、インラインで埋め込まれるオブジェクトのコピーと、外部リソースとして参照される W e b ページの H T M L 文書又はオブジェクトのコピーとに対し、電子証明書をタイムスタンプ証明書発行機能 7 1 から取

得（ステップ S 7 3）する。保存機能 1 5 9 は、例えば、電子証明書により日時と共にユニークに特定且つ認証された情報の全てを記憶装置 6 1' に格納（ステップ S 7 5）する。なお、Web ページの HTML 文書のコピーを記憶装置に保存するかは任意である。そして、この処理を記録終了の条件が満たされるまで繰り返す（ステップ S 7 7）。記録終了の条件とは、例えば依頼人 A の指定した記録期間が終了した場合や、依頼人 A の指定した記録回数に達した場合等である。

【 0 0 2 2 】

図 8 で説明したコピー取得処理を図 9 を用いてもう少し詳しく説明しておく。まず、依頼人 A による指定アクセス先 Web ページの HTML 文書のコピーを取得（ステップ S 9 3）する。そして、この指定アクセス先 Web ページの HTML 文書のコピーを解析し、インラインで埋め込まれたオブジェクトが含まれるかどうか検査（ステップ S 9 5）する。もし、オブジェクトが含まれる場合には、当該オブジェクトのコピーも取得（ステップ S 9 7）する。一方、オブジェクトが含まれない場合にはステップ S 9 9 に移行する。

次に、Web ページ又はオブジェクトへのリンクが存在するか判断（ステップ S 9 9）する。存在する場合には、リンク先の Web ページの HTML 文書又はオブジェクトのコピーを取得（ステップ S 1 0 1）する。一方、存在しない場合には、処理を終了する。なお、図 9 では指定アクセス先 Web ページの 1 階層下の Web ページ又はオブジェクトまでをコピー取得の範囲としているが、もし、これ以下の階層の Web ページ又はオブジェクトをコピー取得の範囲とする場合には、参照先 Web ページをステップ S 9 3 の指定アクセス先とみなして図 9 の処理を実施する。その際、ある階層以下のリンク先を取得対象としない場合には、ステップ S 9 9 及び S 1 0 1 を実施せずに処理を終了すれば良い。

このようにして取得及び生成した情報に対して電子証明書を取得するわけであるが、図 4 で述べたような電子証明書を取得する場合には、最初に生成すべきハッシュ値の計算には以下のような態様が考えられる。図 1 0 に示したように、インラインでオブジェクトが埋め込まれており、外部リソースを参照していない場合には、アクセス先 Web ページの HTML 文書のファイルと、オブジェクトのファイル（場合によっては複数のオブジェクトが存在する。図 1 0 ではオブジェ

クト 1 及びオブジェクト 2 の 2 つを示した。) と、属性情報のファイルと、変更されている HTML 文書のファイルについて、合わせてハッシュ値を 1 つ生成することも考えられる。これにより電子証明書は 1 つ取得される。

また、図 1 1 に示すように、インラインでオブジェクトが埋め込まれており、外部リソースを参照している場合には、アクセス先 Web ページの HTML 文書のファイルと、オブジェクトのファイルと、属性情報のファイルと、変更されている HTML 文書のファイルと、参照先の HTML 文書又はオブジェクトのファイルとについて、合わせてハッシュ値を 1 つ生成することも考えられる。これにより電子証明書は 1 つ取得される。

さらに図 1 2 に示すように、インラインでオブジェクトが埋め込まれており、外部リソースを参照している場合には、アクセス先 Web ページの HTML 文書のファイルと、オブジェクトのファイルと、属性情報のファイルと、変更されている HTML 文書のファイルとに対して、合わせてハッシュ値を生成し、参照先の Web ページの HTML 文書又はオブジェクトのファイルと、その参照先 Web ページの HTML 文書に対する属性情報とに対して 2 番目のハッシュ値を生成する場合も考えられる。このようにすると、参照先 Web ページの HTML 文書についても独立した電子証明書が発行されることになるので、別個にネットワーク上公開されていたことを証明することができるようになる。

なお、上の説明では、インラインで埋め込まれるオブジェクトと外部リソースとして参照される Web ページ又はオブジェクトとを両方取得することにしてしたが、依頼人 A の指示によりいずれかにすることも可能である。さらに、外部リソースとして参照される Web ページについてはさらに下の階層が参照先として存在する可能性があるが、これについての取り扱いも依頼人 A の指示に従う。もし、依頼人 A が何らの指示も出さない場合には、例えば 1 階層下までを取得するという原則的なルールに従っても良い。さらに、参照先 Web ページにもオブジェクトがインラインで埋め込まれている場合があり、その場合にはオブジェクトも参照先 Web ページに含まれるものとして取り扱う場合もある。

【 0 0 2 3 】

図 1 3 に記録内容提供依頼に応じた処理を示しておく。まず、証明書提供機能

1 6 1 は、依頼人 A の記録内容提供依頼から証明対象電子情報を特定（ステップ S 8 1）する。そして、対象電子情報のコピーと、電子証明書と、属性情報と、インラインで埋め込まれたオブジェクトと、参照先オブジェクト又は電子情報と、対象電子情報の変形されたコピーとを、記憶装置 6 1' から読み出し、C D - R 6 3' 等により提供（ステップ S 8 5）する。上で述べたサービス（5）における記録内容提供依頼でも同じように図 1 3 の処理が実施される。

以上述べた内容は一例であって様々な変形が可能である。例えば、5' で示すサーバ B に含まれる 6 つの機能は 1 つの 5' で示すサーバ B に含まれるように図 7 では示しているが、複数のサーバに分けて存在するようにすることも可能である。同様に、9 で示すサーバ D では、依頼された W e b ページへのリンクを掲載し、且つ検索機能を設けているが、これらも別個のサーバにて実施されるようにすることも可能である。ネットワーク 1 に接続される一般公衆向け検索エンジンは 1 つに限定されない。また、h t t p に限定されず、f t p でも対応することができる。7 で示すサーバ C の機能を 5 で示すサーバ B の機能に含めることも可能である。7 で示すサーバ C によるサービスを行う主体と、5' で示すサーバ B によるサービスを行う主体は、別でも同一でもよい。ネットワーク 1 はインターネットに限定されず、他の非排他的なアクセスを許可するネットワーク及びネットワーク利用を希望する者が非排他的に取り扱われるネットワークに拡大可能である。記録内容提供のための媒体を C D - R としていたが、これも一例であって他の媒体、例えば C D - R O M でも、D V D でもよい。

また図 1 に示した機能ブロックの分け方は一例であって、1 つの機能ブロックを複数の機能ブロックに分けることも、複数の機能ブロックを 1 つの機能ブロックにまとめることも可能である。図 1 及び図 7 に示した機能ブロックの機能を実現するプログラムとコンピュータの組み合わせにより図 1 及び図 7 のような装置を構成することも、一部又は全部を専用の電子回路等により実施することも可能である。

【0 0 2 4】

【発明の効果】

本発明により、インターネット等のネットワーク上で、ある電子情報が所定の

条件の下公開されていたこと及びある電子情報のオンラインにおける情報伝達状態を証明するための方法、システム及びコンピュータ・プログラム並びに該コンピュータ・プログラムを格納した記録媒体を提供することができた。

【図面の簡単な説明】

【図 1】

本発明におけるシステムの概要を示すブロック図である。

【図 2】

電子情報記録依頼に応じて行われる処理の一例を示すフローチャートである。

【図 3】

記録内容提供依頼に応じて行われる処理の一例を示すフローチャートである。

【図 4】

電子情報を日時と共に特定し且つ認証する電子証明書の発行処理の一例を示す模式図である。

【図 5】

オンラインで Web ページを閲覧した場合の表示画面例である。

【図 6】

オフラインで Web ページを閲覧した場合の表示画面例である。

【図 7】

図 1 のサーバ B (5) をサーバ B (5 ') に変更する場合の機能ブロック図である。

【図 8】

電子情報記録依頼に応じて行われる処理の一例を示すフローチャートである。

【図 9】

図 8 のコピー取得ステップの詳細なフローチャートである。

【図 1 0】

ハッシュ値計算の一例を示す模式図である。

【図 1 1】

ハッシュ値計算の一例を示す模式図である。

【図 1 2】

ハッシュ値計算の一例を示す模式図である。

【図 1 3】

記録内容提供依頼に応じて行われる処理の一例を示すフローチャートである。

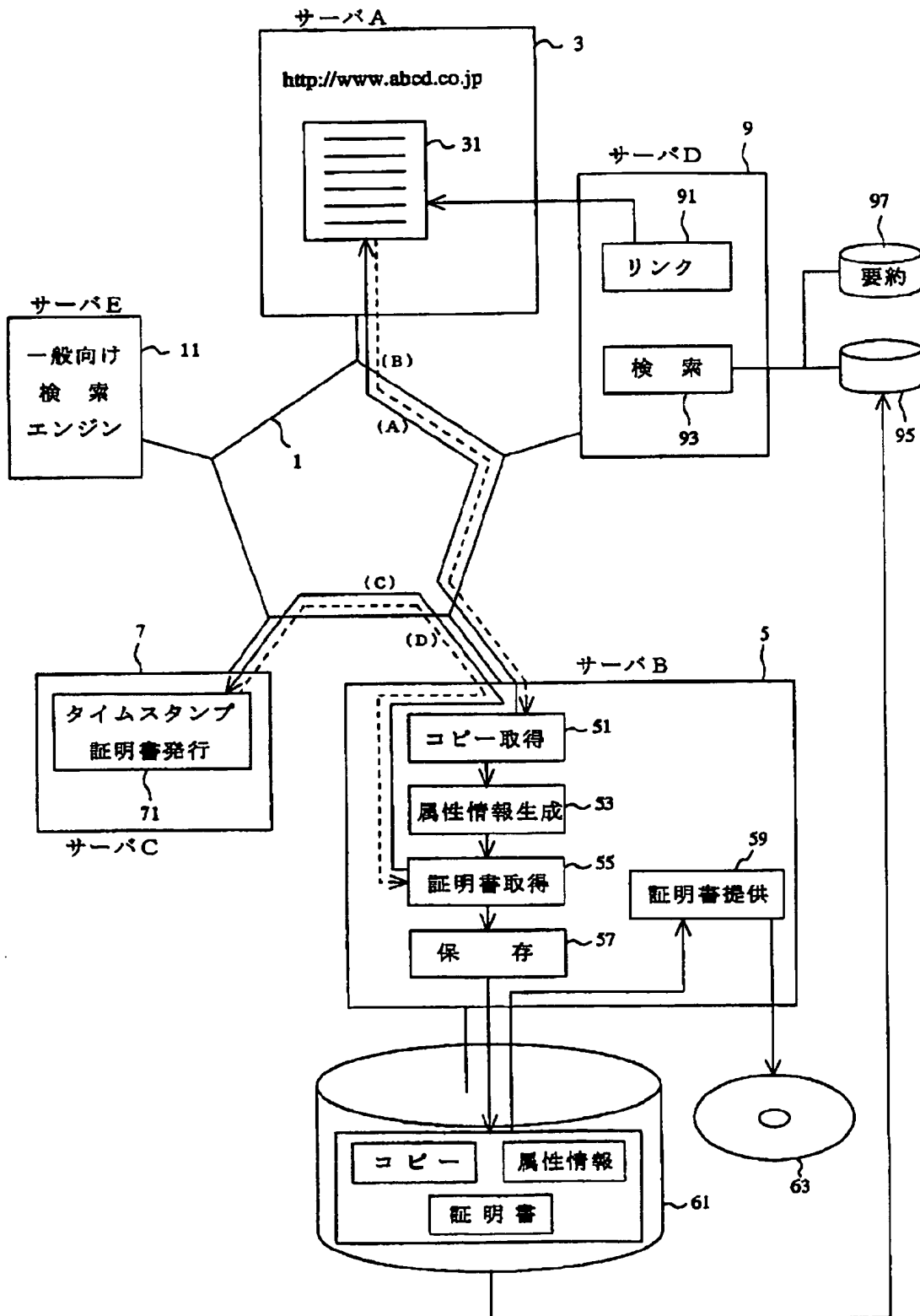
【符号の説明】

- 1：ネットワーク
- 3：サーバA
- 5：サーバB 5'：サーバB
- 7：サーバC
- 9：サーバD
- 11：サーバE
- 31：Web ページ
- 51：コピー取得機能
- 53：属性情報生成機能
- 55：証明書取得機能
- 57：保存機能
- 59：証明書提供機能
- 61：記憶装置 61'：記憶装置
- 63：CD-R 63'：CD-R
- 71：タイムスタンプ証明書発行機能
- 91：リンク
- 93：検索機能
- 97：要約データベース
- 151：コピー取得機能
- 153：コピー変形機能
- 157：証明書取得機能
- 159：保存機能
- 161：証明書提供機能

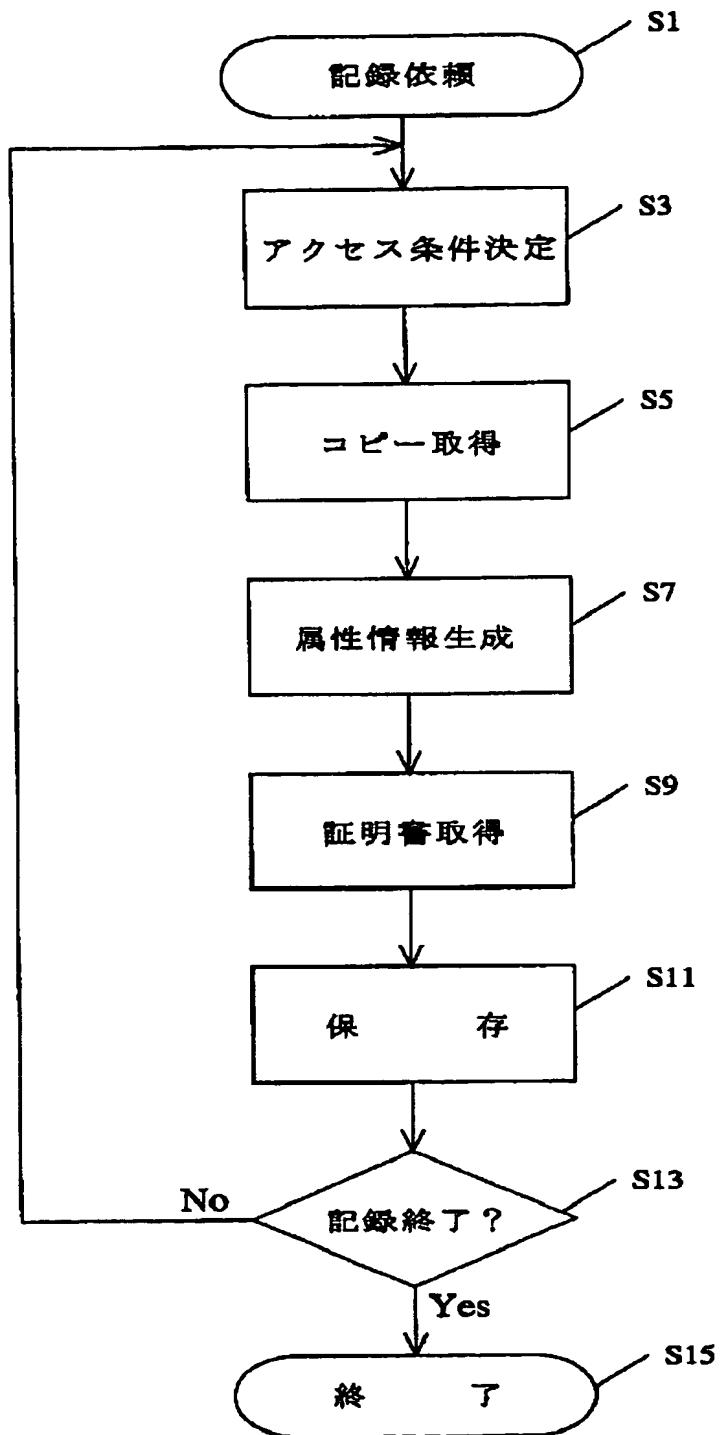
【書類名】

図面

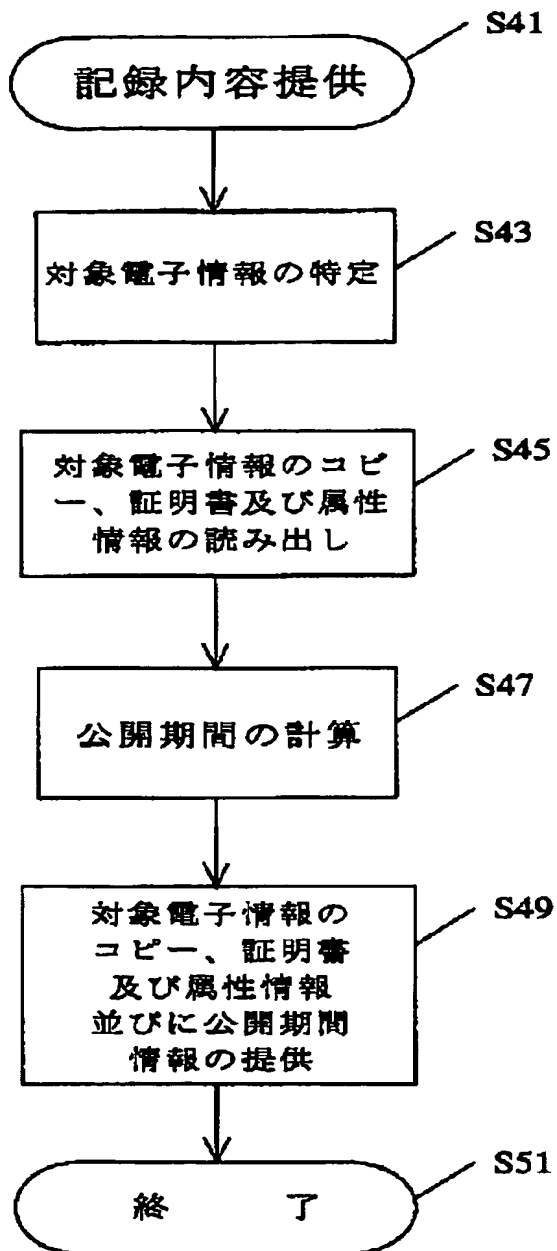
【図 1】



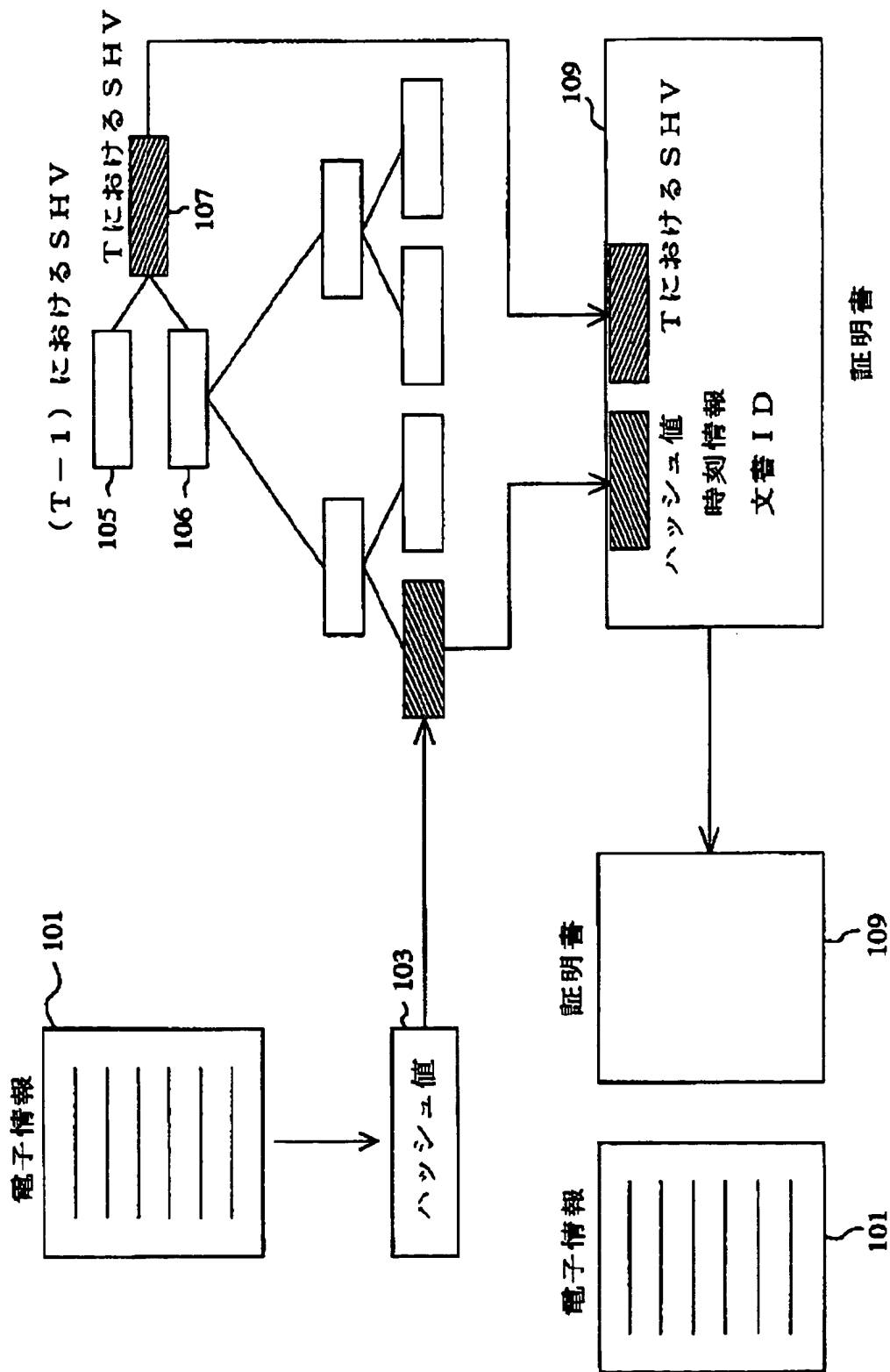
【図 2】



【図 3】

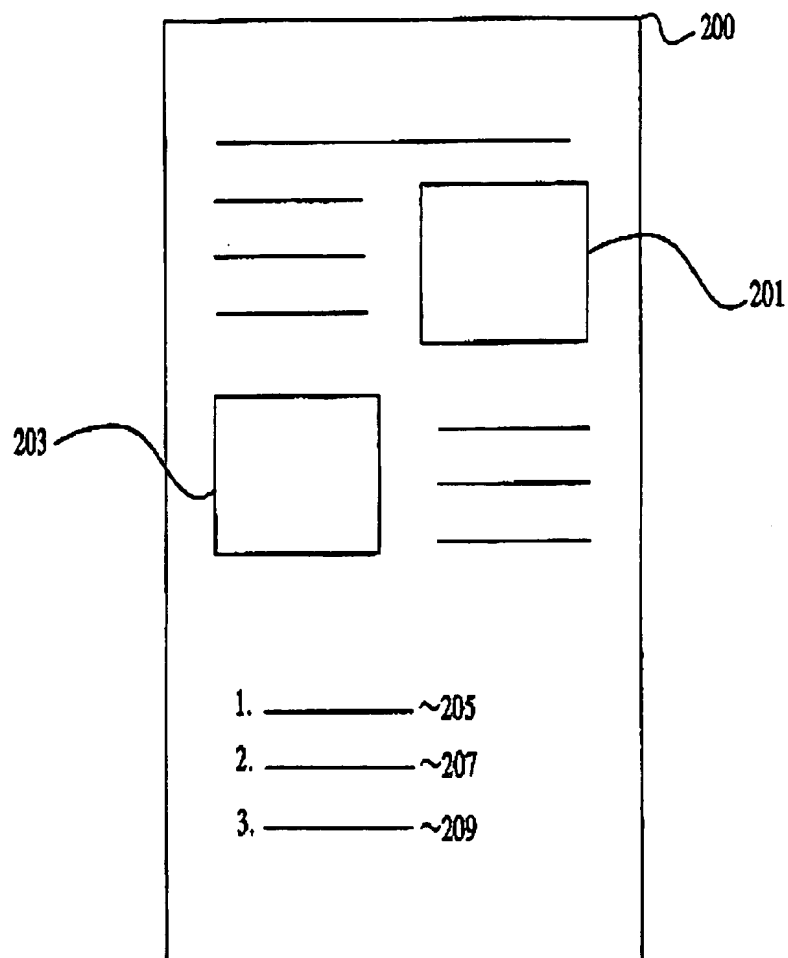


【図 4】



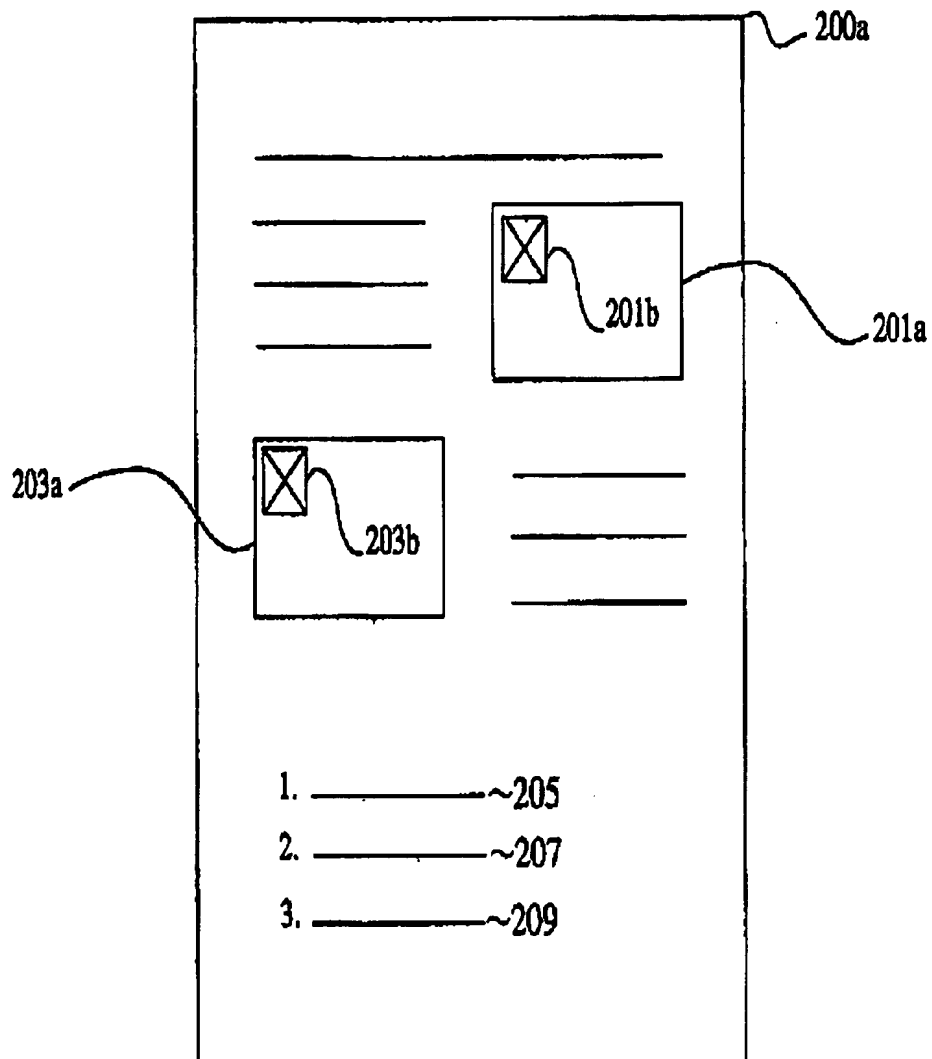
【図 5】

オンライン時の表示例

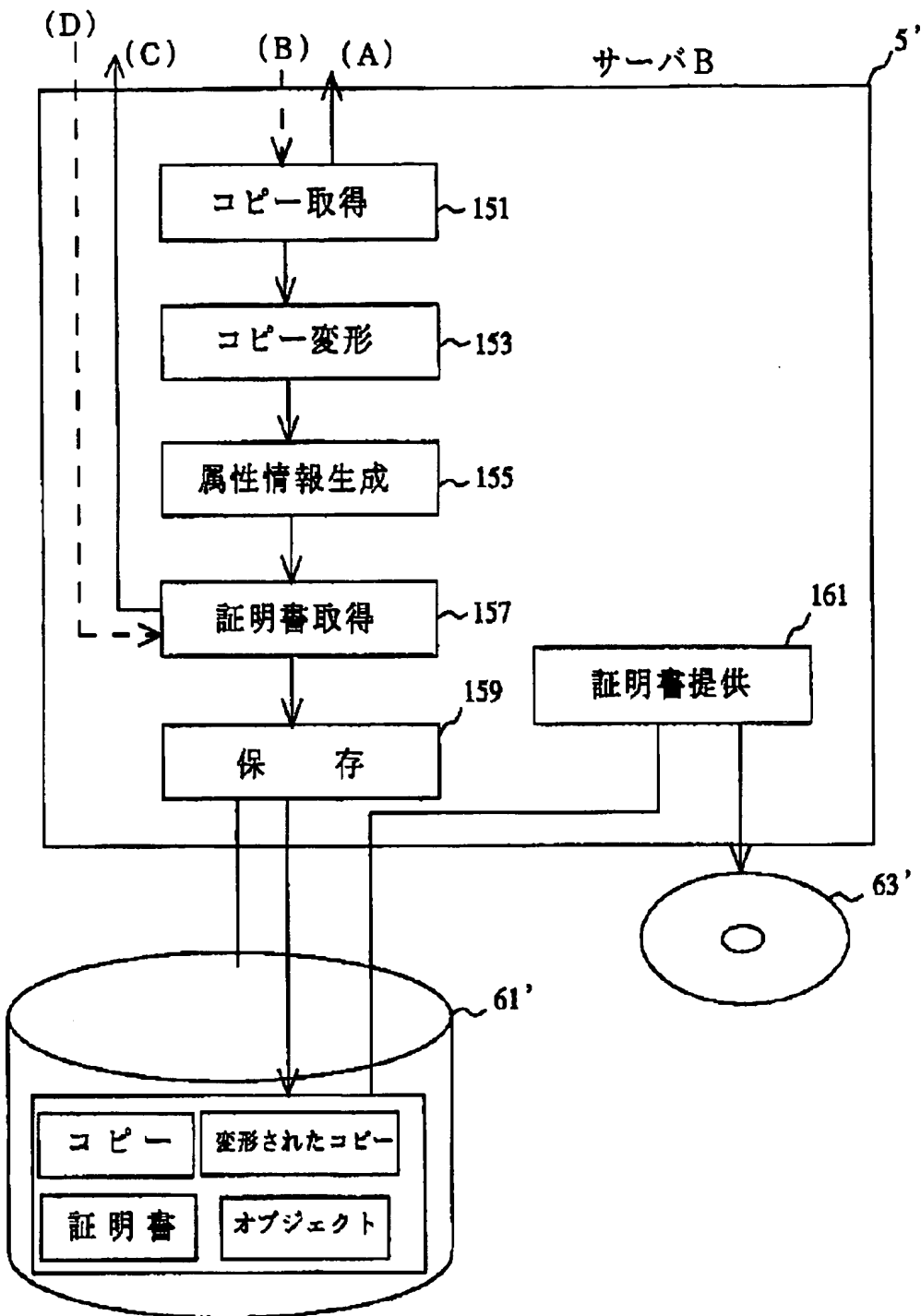


【図 6】

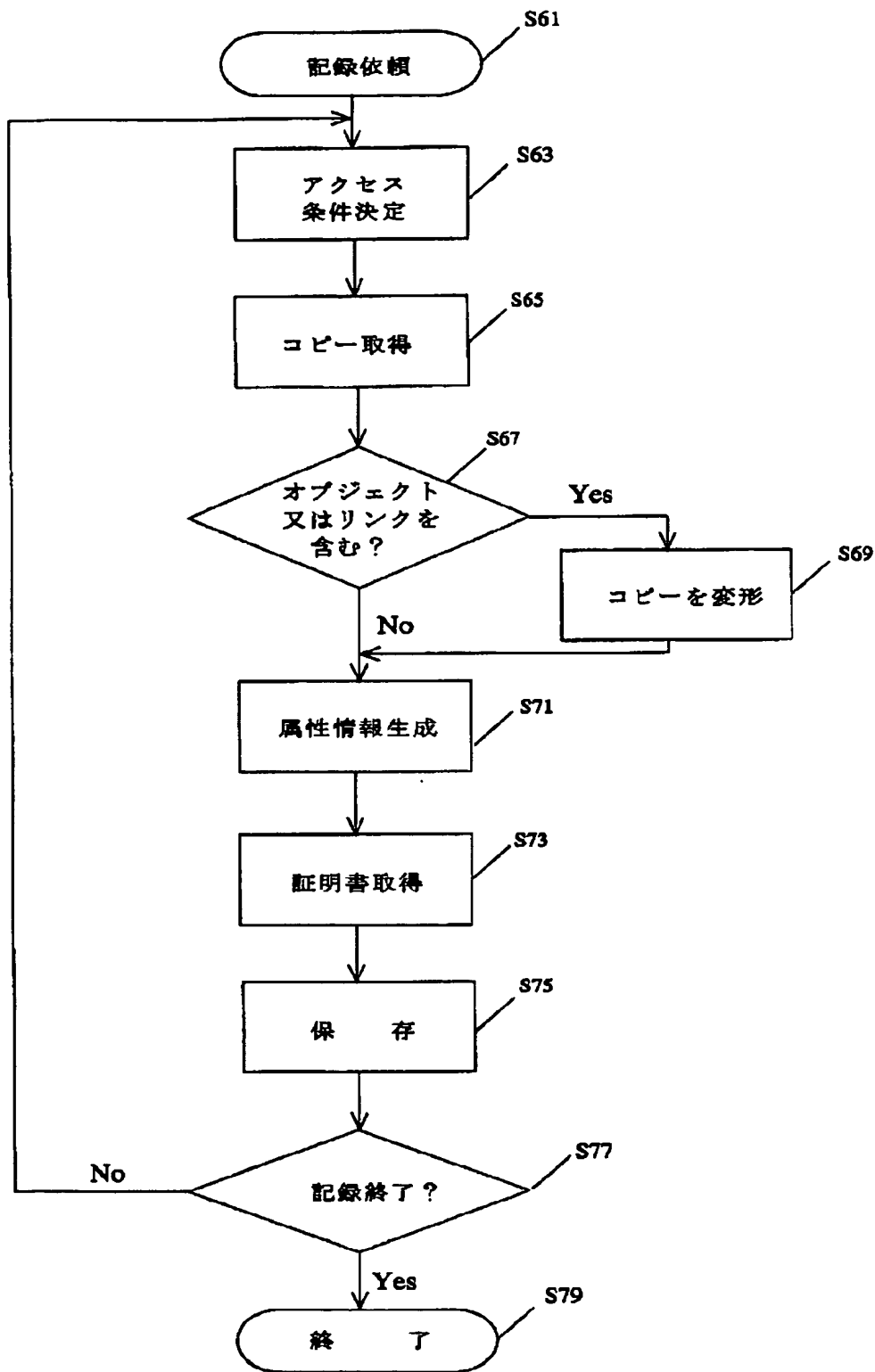
ローカルに保存した場合の表示例



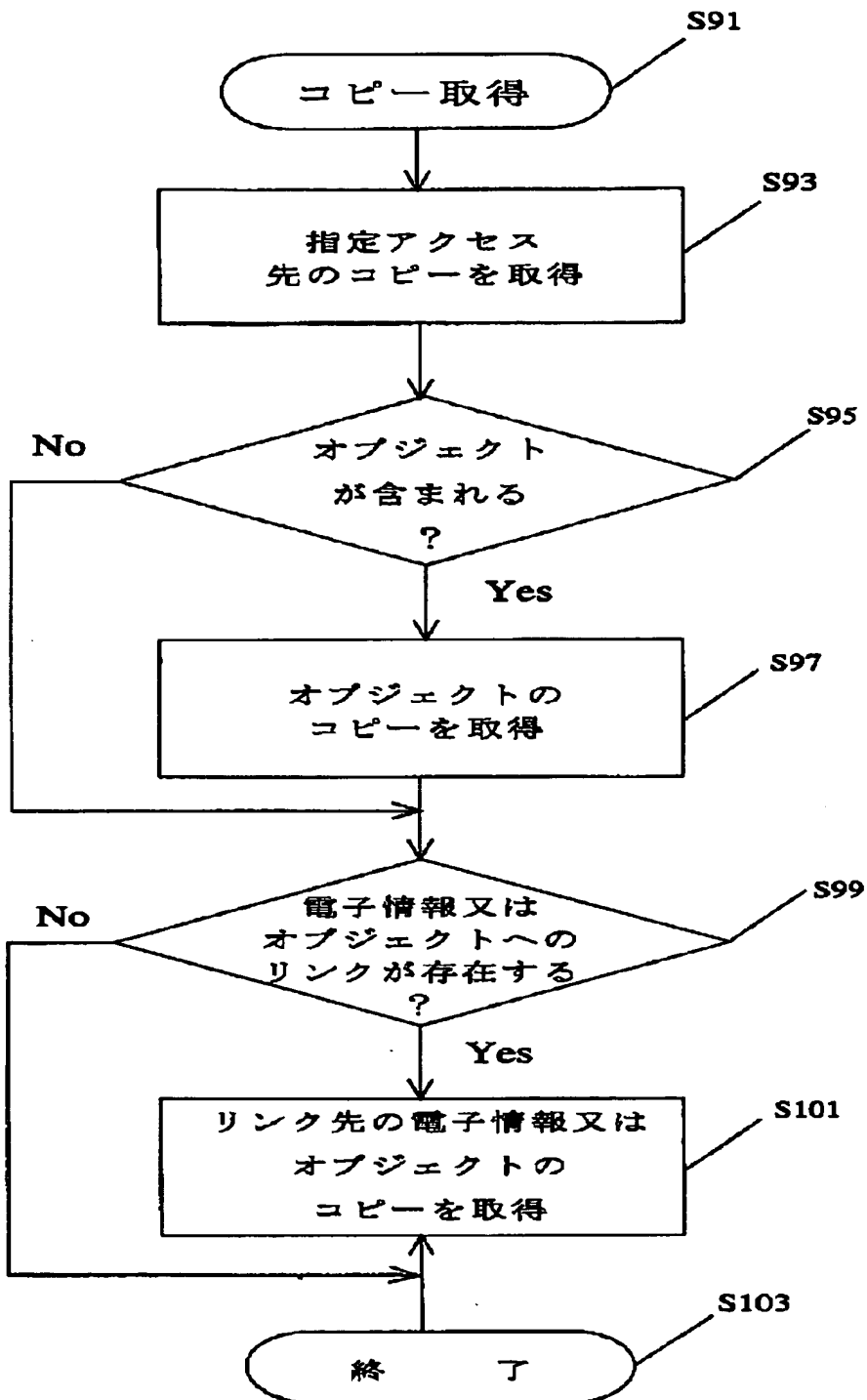
【図 7】



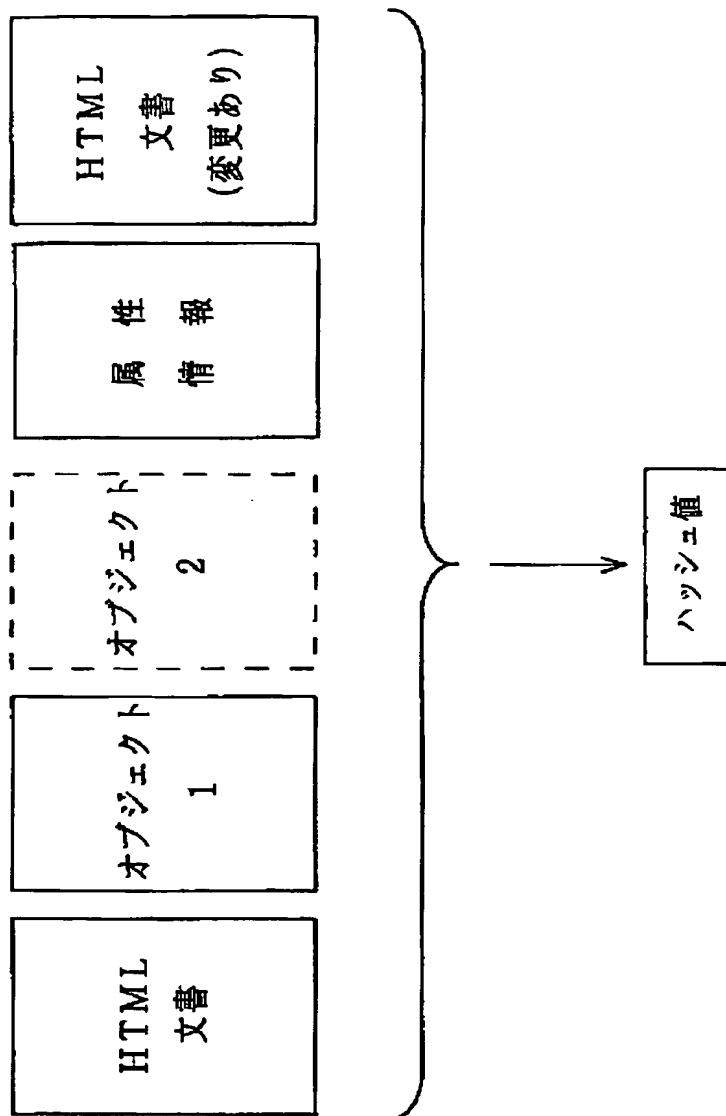
【図 8】



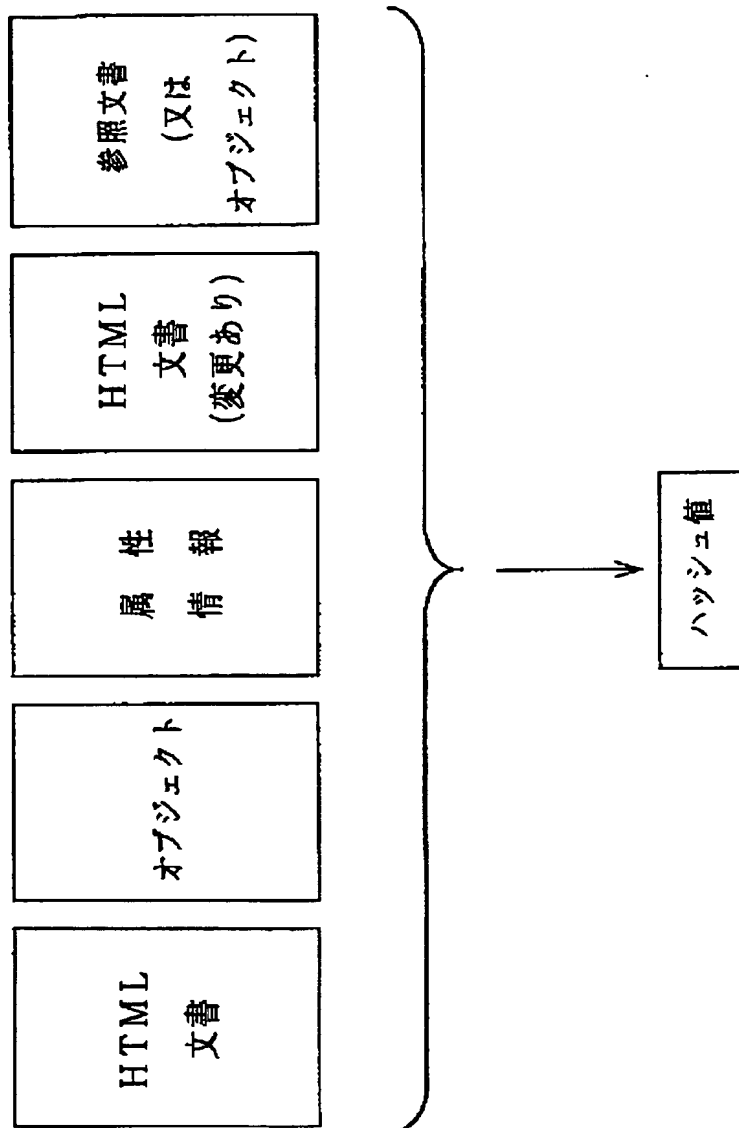
【図 9】



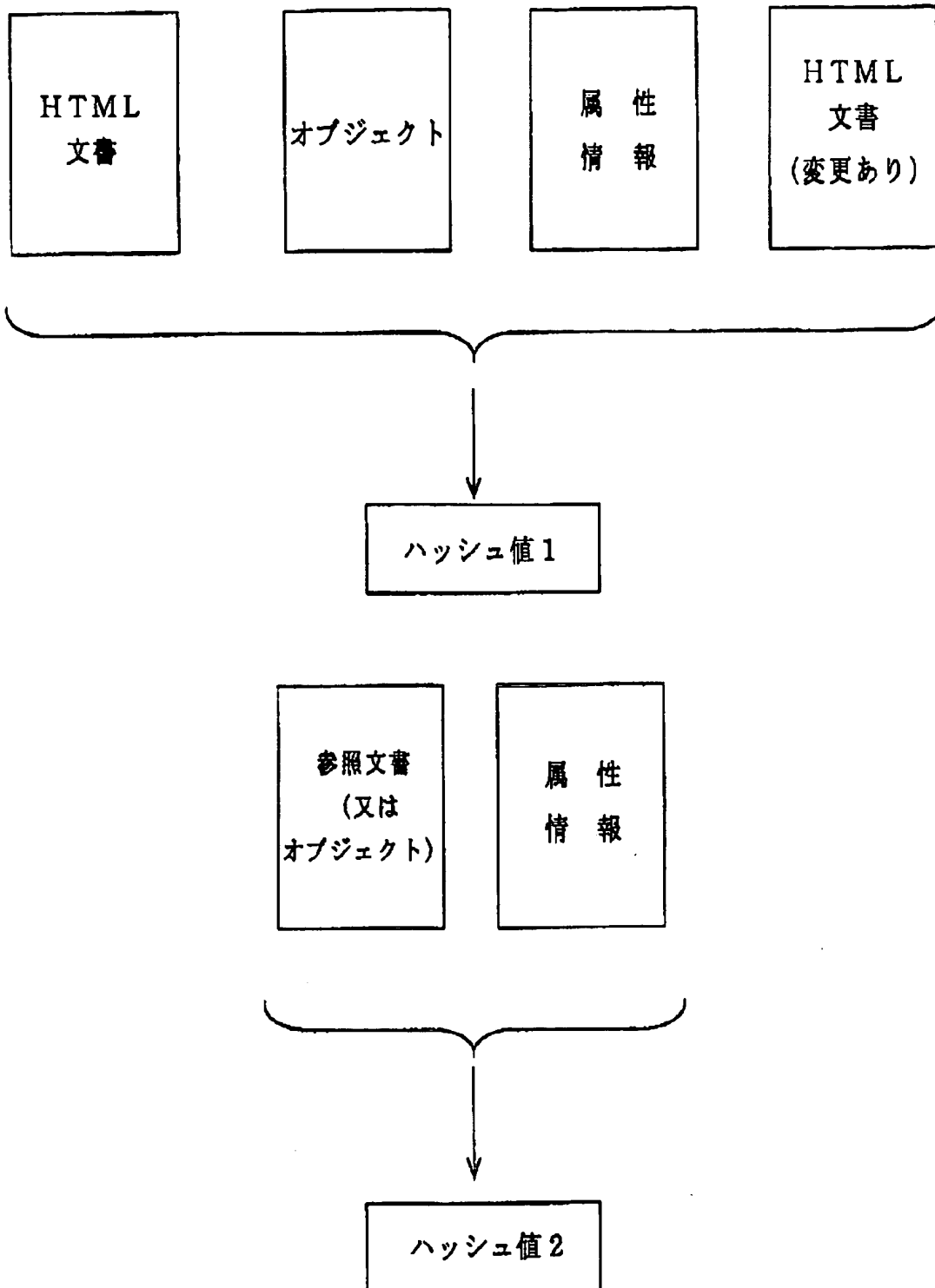
【図 1 0】



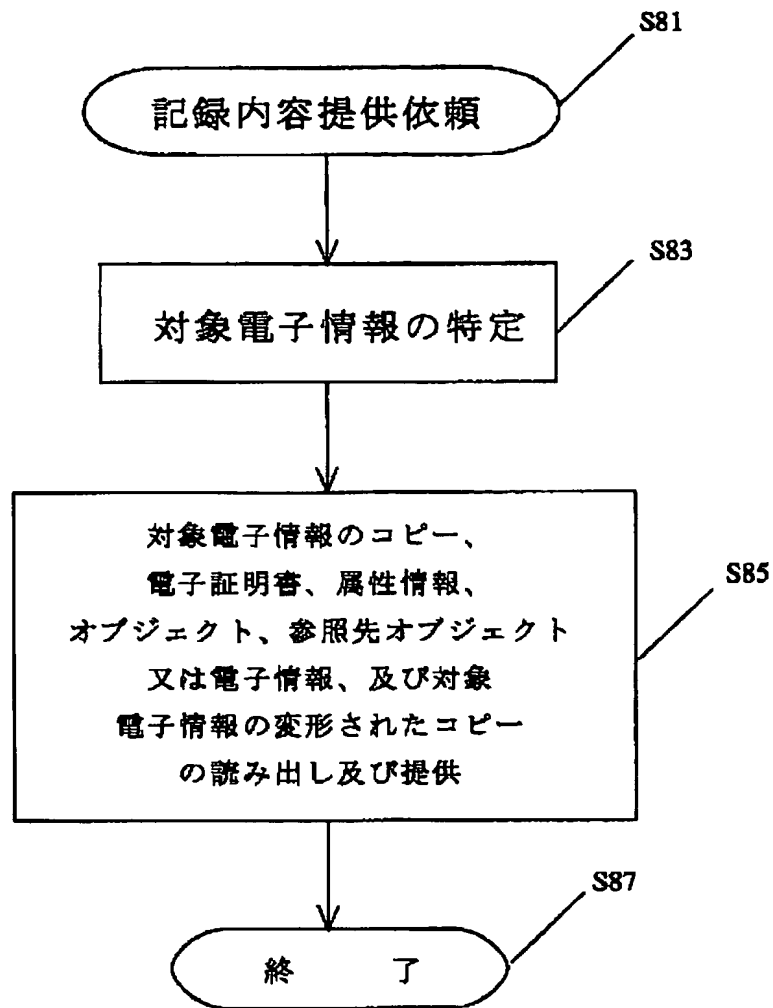
【図 1 1】



【図 1 2】



【図 1 3】



【書類名】 要約書

【要約】

【課題】 インターネット等のネットワーク上で、特定の電子情報が所定の条件の下公開されていたこと及び特定の電子情報のオンラインにおける情報伝達状態を証明すること。

【解決手段】 記録依頼に応じて、特定のコンピュータに格納された特定の電子情報にアクセスし、特定の電子情報及び当該特定の電子情報に含まれるオブジェクトをコピーする。次に、特定の電子情報及びオブジェクトをローカルに保存した場合にローカルに保存された特定の電子情報からオブジェクトを利用可能なように特定の電子情報を変更し、変更された特定の電子情報をコピーされたオブジェクトと共に記憶装置に格納する。コピーされた特定の電子情報及びオブジェクトと、変更された特定の電子情報と、特定の電子情報の所在に関する情報を含む属性情報とを日時と共にユニークに特定し且つ認証する電子証明書を取得する。電子証明書等により公開されていたこと及び情報伝達状態を証明できる。

【選択図】 図 8

特願平 1 1 - 3 4 1 2 8 9

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 6 7 4 7]

- | | |
|----------|------------------------|
| 1. 変更年月日 | 1 9 9 0 年 8 月 2 4 日 |
| [変更理由] | 新規登録 |
| 住 所 | 東京都大田区中馬込 1 丁目 3 番 6 号 |
| 氏 名 | 株式会社リコー |
| | |
| 2. 変更年月日 | 2 0 0 2 年 5 月 1 7 日 |
| [変更理由] | 住所変更 |
| 住 所 | 東京都大田区中馬込 1 丁目 3 番 6 号 |
| 氏 名 | 株式会社リコー |